STATE OF SOUTH DAKOTA
OFFICE OF PROCUREMENT MANAGEMENT
523 EAST CAPITOL AVENUE
PIERRE, SOUTH DAKOTA 57501-3182

TRANSCRIPTION SERVICES REQUEST FOR PROPOSAL

PROPOSALS ARE DUE NO LATER THAN June 20, 2019 at 5:00pm CDT

RFP #1695

BUYER: Division of Human Services Center

POC: Dawson Lewis
Dawson.Lewis@state.sd.us

READ CAREFULLY

FIRM NAME: _____ AUTHORIZED SIGNATURE: _____

ADDRESS: _____ TYPE OR PRINT NAME: _____

CITY/STATE: _____ TELEPHONE NO: _____

ZIP (9 DIGIT): _____ FAX NO: _____

FEDERAL TAX ID#: _____ E-MAIL: _____

PRIMARY CONTACT INFORMATION

CONTACT NAME: _____ TELEPHONE NO: _____

FAX NO: _____ E-MAIL: _____

1.0 GENERAL INFORMATION

1.1 PURPOSE OF REQUEST FOR PROPOSAL (RFP)

The South Dakota Department of Social Services (DSS), Human Services Center (HSC), issues this RFP to identify and select a qualified Contractor able to provide transcription services for HSC.

1.2 ISSUING OFFICE AND RFP REFERENCE NUMBER

The South Dakota Human Services Center (HSC) is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota, Department of Social Services. The reference number for the transaction is RFP #1695. Refer to this number on all proposals, correspondence, and documentation relating to the RFP.

Please refer to the Department of Social Services website link http://dss.sd.gov/keyresources/rfp.aspx for the RFP, any related questions/answers, changes to schedule of activities, amendments, etc

1.3 LETTER OF INTENT

All interested offerors are requested to submit a non-binding **Letter of Intent** to respond to this RFP. While preferred, a Letter of Intent is not mandatory to submit a proposal.

The letter of intent must be received by email in the Department of Social Services by no later than May 30, 2019 and must be addressed to Sandra.Barkley@state.sd.us. Place the following, exactly as written, in the subject line of your email: **Letter of Intent for RFP #1695.** Be sure to reference the RFP number in any attached letter or document.

1.4 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Publication	May 16, 2019
Letter of Intent to Respond Due	May 30, 2019
Deadline for Submission of Written Inquiries	May 30, 2019
Responses to Offeror Questions	June 6, 2019
Proposal Submission	June 20, 2019
Anticipated Award Decision/Contract Negotiation	July 9,2019

1.5 SITE VISITS

It is not anticipated that site visits will be needed for this RFP

1.6 SUBMITTING YOUR PROPOSAL

All proposals must be completed and received at the HSC by the date and time indicated in the Schedule of Activities.

Proposals received after the deadline will be late and ineligible for consideration.

An original, four (4) identical copies, and one (1) digital, Portable Document Format (PDF) copy loaded on a USB flashdrive of the proposal, all attachments, and the cost proposal(s) must be submitted.

All proposals must be signed in ink by an officer of the offeror legally authorized to bind the offeror to the proposal, and sealed in the form intended by the respondent. Proposals that are not properly signed may be rejected. The sealed envelope must be marked with the appropriate RFP Number and Title. The words "Sealed Proposal Enclosed" must be prominently denoted on the outside of the shipping container. **Proposals must be addressed and labeled as follows:**

Request For Proposal #1695 Proposal Due 5:00 PM CDTJune 20, 2019
South Dakota Department of Social Services
Attention: Sandy Barkley
3615 Broadway
PO Box 7600
Yankton SD 57078-7600

No punctuation is used in the address. The above address as displayed should be the only information in the address field.

No proposal may be accepted from, or any contract or purchase order awarded to any person, firm or corporation that is in arrears upon any obligations to the State of South Dakota, or that otherwise may be deemed irresponsible or unreliable by the State of South Dakota.

1.7 CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION – LOWER TIER COVERED TRANSACTIONS

By signing and submitting this proposal, the offeror certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation, by any Federal department or agency, from transactions involving the use of Federal funds. Where the offeror is unable to certify to any of the statements in this certification, the bidder shall attach an explanation to their offer.

1.8 NON-DISCRIMINATION STATEMENT

The State of South Dakota requires that all contractors, vendors, and suppliers doing business with any State agency, department, or institution, provide a statement of non-discrimination. By signing and submitting their proposal, the offeror certifies they do not discriminate in their employment practices with regard to race, color, creed, religion, age, sex, ancestry, national origin or disability.

1.9 MODIFICATION OR WITHDRAWAL OF PROPOSALS

Proposals may be modified or withdrawn by the offeror prior to the established due date and time.

No oral, telephonic, telegraphic or facsimile responses or modifications to informal, formal bids, or Request for Proposals will be considered.

1.10 OFFEROR INQUIRIES

Offerors may email inquiries concerning this RFP to obtain clarification of requirements. No inquiries will be accepted after 5:00 PM CDT May 30, 2019. Email inquiries must be sent to **Sandra.Barkley@state.sd.us** with the following wording, exactly as written, in the subject line: **RFP #1695 Questions**.

The Department of Social Services (DSS) will respond to offerors' inquiries by posting offeror aggregated questions and Department responses on the DSS website at http://dss.sd.gov/keyresources/rfp.aspx no later than June 6, 2019. For expediency, DSS may combine similar questions. Offerors may not rely on any other statements, either of a written or oral nature, that alter any specification or other term or condition of this RFP. Offerors will be notified in the same manner as indicated above regarding any modifications to this RFP.

1.11 PROPRIETARY INFORMATION

The proposal of the successful offeror(s) becomes public information. Proprietary information can be protected under limited circumstances such as client lists and non-public financial statements. Pricing and service elements are not considered proprietary. An entire proposal may not be marked as proprietary. Offerors must clearly identify in the Executive Summary and mark in the body of the proposal any specific proprietary information they are requesting to be protected. The Executive Summary must contain specific justification explaining why the information is to be protected. Proposals may be reviewed and evaluated by any person at the discretion of the State. All materials submitted become the property of the State of South Dakota and may be returned only at the State's option.

1.12 LENGTH OF CONTRACT

This RFP may result in a single or multiple award contract. The term of the contract shall be one year, beginning August 1, 2019 or as soon thereafter as possible, with the option to renew, in one (1) year increments, for four (4) additional one (1) year extensions at HSC's discretion and by mutual agreement of the parties.

1.13 GOVERNING LAW

Venue for any and all legal action regarding or arising out of the transaction covered herein shall be solely in Hughes County, State of South Dakota. The laws of South Dakota shall govern this transaction.

1.14 DISCUSSIONS WITH OFFERORS (ORAL PRESENTATION/NEGOTIATIONS)

An oral presentation by an offeror to clarify a proposal may be required at the sole discretion of the State. However, the State may award a contract based on the initial proposals received without discussion with the offeror. If oral presentations are required, they will be scheduled after the submission of proposals. Oral presentations will be made at the offeror's expense.

This process is a Request for Proposal/Competitive Negotiation process. Each Proposal shall be evaluated, and each respondent shall be available for negotiation meetings at the State's request. The State reserves the right to negotiate on any and/or all components of every proposal submitted. From the time the proposals are submitted until the formal award of a contract, each proposal is considered a working document and as such, will be kept confidential. The negotiation discussions will also be held as confidential until such time as the award is completed.

2.0 STANDARD AGREEMENT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include, at minimum, the State's standard terms and conditions as seen in Attachment A. As part of the negotiation process, the contract terms listed in Attachment A may be altered or deleted. The offeror should indicate in their response any issues they have with any specific contract terms. If the offeror does not indicate any contract term issues, then the State will assume the terms are acceptable.

3.0 SCOPE OF WORK

The offeror's proposal must provide responses or acknowledgements (as appropriate) indicating how each of the following requirements can or cannot be met.

3.1 TECHNOLOGY

3.1.1 Transcription service will use same electronic platform as HSC's voice recognition software within HSC's electronic health record, M Modal. Transcription service using the same platform will increase efficiency of speech recognition software within our electronic medical record and essentially train the upfront speech recognition product as the dictation is being typed.

3.1.2 Transcription service will fully interface with the electronic health record, MyAvatar, by Netsmart Technologies' electronic health record (EHR) system.

3.1.3 Transcription service will use an API interface method to allow for direct entry into the EHR.

3.1.4 The offeror's solution must provide a portal to allow HSC staff to listen to voice files and edit documents within the transcription system.

3.1.5 Transcription service must offer a toll free number for HSC providers to dictate.

3.1.6 Transcription service must offer a mobile application for smart devices with documented HIPAA compliance safeguards in place.

3.2 UNITS OF MEASURE

The Vendor will use the following definitions:

3.2.1 65 Character ASCII Line with Headers and Footers ("65-char ASCII w/H&F"): ASCII characters 0-225 within the formatted document including Microsoft Word defined headers and footers, which are areas in the top and bottom margins of each page in a document, divided by 65. No more than two consecutive spaces or tabs are counted.

3.2.2 Report: A fully transcribed structured text document representing a medical report in a format agreed upon by the parties.

3.3 MINIMUM TRANSCRIPTION SERVICE STANDARDS

3.3.1 Transcription service must fully interface with electronic health record, MyAvatar, by Netsmart Technologies.

3.3.2 Document types will flow directly into the EHR via interface with a queue to allow for staff to edit and approve, and send to physician workload (to do list).

3.3.3 Transcription service must provide transcribed documents with turnaround time of 3 hours to 24 hours, depending upon document type, at the same fee.

3.4 **STAT REQUESTS**

Transcription service must provide service of turnaround time of less than 2 hours for stat requests. This must be at no additional cost for up to 2.99% of the documents typed requested as a stat report.

3.5 **DATA INTERRUPTION HANDLING**

When the connection between the offerors servers and MyAvatar on the State's servers is lost;

3.5.1 Describe how the system ensures that a file is completely uploaded when interrupted partially through the transfer.

3.5.2 If a whole file is not able to be transferred, describe how the system ensures that it is transmitted at a later time.

3.6 **TRAINING AND SUPPORT**

3.6.1 Transcription service must offer a toll free number for HSC providers to dictate.

3.6.2 The Transcription service must provide onsite training and subject matter experts to assist in the adoption of the service at a maximum of fifteen (15) hours.

3.7 **HOURS OF OPERATION**

Transcription service must have hours of operation twenty four hours per day, seven days a week, excluding scheduled maintenance.

3.8 **SCHEDULED MAINTENACE**

Transcription service shall not allocate more than 10 hours per month for Scheduled Maintenance.

3.8.1 Scheduled Maintenance must be communicated to South Dakota HSC with not less than 48 hours notice and completed during non-peak work times. These non-work times will be agreed upon with HSC staff.

3.9 **FAMILIARITY WITH HSC AND DSS**

Consideration will be given to offerors knowledgable of the policies and procedures enforced at HSC, and how those work within the overall HIPAA framework.

4.0 PROPOSAL REQUIREMENTS AND COMPANY QUALIFICATIONS

4.1 The offeror is cautioned that it is the offeror's sole responsibility to submit information related to the evaluation categories and that the State of South Dakota is under no obligation to solicit such information if it is not included with the proposal. The offeror's failure to submit such information may cause an adverse impact on the evaluation of the proposal.

4.2 **Offeror's Contacts**: Offerors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct all of their questions or comments regarding the RFP, the evaluation, etc. to the point of contact of the buyer of record indicated on the first page of this RFP. Offerors and their agents may not contact any state employee other than the buyer of record regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension and/or exclusion from specific procurements. Offerors and their agents who have questions regarding this matter should contact the buyer of record.

4.3 The offeror must provide the following information related to at least three previous and current service/contracts performed by the offeror's organization which are similar to the requirements of this RFP. Provide this information for any service/contract that has been terminated, expired or not renewed in the past three years:

– –

a. Name, address and telephone number of client/contracting agency and a representative of that agency who may be contacted for verification of all information submitted;
b. Dates of the service/contract; and
c. A brief, written description of the specific prior services performed and requirements thereof.

4.4 The selected offeror will be required to provide a copy of its most recent System and Organization Controls, Statement on Standards for Attestation Engagements (SOC 1 SSAE18) report, then annually thereafter for the term of the agreement. For SOC 1 SSAE 18 the offeror must identify which of the following can be provided on an annual basis: SOC 1, SOC 2, or SOC 3. If unable to provide a copy of the most recent report, offeror must explain why and whether in the future the selected offeror will be able to provide a report.

4.5 Offeror must complete and submit with their proposal Attachment D, the South Dakota Bureau of Information & Telecommunications (BIT) Technology Security and Vendor Questions.

4.6 The offeror must acknowledge that if selected, they must sign and return the Security Acknowledgement (Attachment A, Exhibit C) prior to contract finalization and read the Information Technology Security Policy (ITSP) – Contractor (Attachment A, Exhibit D)

4.7 Documenting the Solution Environment.

4.7.1 If the State will be hosting the solution, the offeror's proposal must include a system diagram. This diagram must be provided as a separate document or attachment to the offeror's proposal. The document must be named "(Your Name) System Diagram and Requirements."

The diagram must be detailed enough that the State can
4.7.1.1 understand the components,
4.7.1.2 the system flow,
4.7.1.3 and system requirements
4.7.1.3.1 The offeror must list the minimum
4.7.1.3.1.1 Software required
4.7.1.3.1.2 Hardware required
4.7.1.3.2 If the offeror's product will not work with the most current versions of server or database software they must list the latest working version.

4.7.2 The offeror must state whether its proposed solution will operate in a virtualized environment. The offeror must also identify and describe all differences, restrictions or limitations of its proposed solution with respect to operation, licensing, support, certification, warranties, and any other details that may impact its proposed solution when hosted in a virtualized environment. This information must be included with the solution diagram for the offeror hosted solution submitted with the offeror's proposal.

4.7.3 If the offeror is hosting the solution, the offeror's proposal must include a diagram providing an overview of the proposed system. This diagram must be provided as a separate document or attachment. The document must be named "(Your Name) Hosted System Diagram."

4.8 All hardware, website(s), or software purchased by the State and deployed on the State's network will be subjected to security scans by BIT.

All solutions acquired by the State that are hosted by the offeror, including Software as a Service, or hosted by a third-party for the offeror will be subjected to security scans by BIT, or

a preapproved detailed security scan report provided by the offeror.

The offeror may submit a security scan report with their proposal for BIT approval, which may be redacted by the offeror. The State's objective is to ascertain whether the contents of the report will be acceptable in lieue of the State conducting a security scan, and is not to review the contents themselves. Approval is not guaranteed. If the scan report is deemed not acceptable, the South Dakota BIT must scan the offeror's solution. The actual security scanning by the State will be performed, or the submission of a security scan report by the offeror will be reviewed for approval, for the proposal to be considered for further review.

The cost of any security scans conducted by the offeror or the offeror's costs associated with the State's scans must be incorporated in the offeror's cost proposal. If the offeror is submitting a security scan report, the offeror should price the product as if the State or the offeror were to perform the security scan.

A detailed security report must consist of at least the following:

- The system that was evaluated (URL if possible, but mask it if needed).
- The categories that were evaluated, *e.g.*, SQL injection, cross site scripting, etc.
- The general findings such as the number of SQL injection issues found, etc.; and the count per category.
- Technical detail of each issue found such as where was it found, *e.g.,* web address, what was found, the http response if possible, etc.

4.9 If the offeror is proposing to use a web application or provide Software as a Service, the most current version of Active Directory Federation Service (ADFS) will be used for all user logins for State of South Dakota Staff, if supported by the offeror.

If the offeror cannot make use of ADFS, the offeror's proposal must explain how State staff will be informed not to use their State password to login to the offeror's solution.

4.10 Background Checks

The offeror must include the following statement in their proposal:

"(Company name here) acknowledges and affirms that it understands that the (company name here) employees who have access to production Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Personal Heath Information (PHI), Federal Tax Information (FTI), any information defined under state statute as confidential, or have access to secure facilities will have fingerprint based background checks.

These background checks will be used to check the criminal history records of the State as well as the Federal Bureau of Investigation's records. (Company name here) acknowledges and affirms that this requirement will extend to include any Subcontractor's, Agents, Assigns and or Affiliated Entities employees."

4.11 The offeror must submit information that demonstrates their availability and familiarity with the locale in which the project (s) are to be implemented.

4.12 The offeror must describe their proposed project management techniques.

4.13 The offeror must detail examples that document their ability and proven history in handling special project constraints

4.14 If an offeror's proposal is not accepted by the State, the proposal will not be reviewed/evaluated.

5.0 PROPOSAL RESPONSE FORMAT

5.1 An original and four (4) copies shall be submitted.

5.1.1 In addition, the offeror must submit one (1) copy of their entire proposal, including all attachments and cost proposal(s), in PDF digital format loaded on a USB flashdrive. Offerors may not send the electronically formatted copy of their proposal via email.

5.1.2 The proposal should be page numbered and should have an index and/or a table of contents referencing the appropriate page number.

5.2 All proposals must be organized and tabbed with labels for the following headings:

5.2.1 **RFP Form**. The State's Request for Proposal form completed and signed.

5.2.2 **Executive Summary.** The one or two page executive summary is to briefly describe the offeror's proposal. This summary should highlight the major features of the proposal. It must indicate any requirements that cannot be met by the offeror. The reader should be able to determine the essence of the proposal by reading the executive summary. Proprietary information requests should be identified in this section.

5.2.3 **Detailed Response.** This section should constitute the major portion of the proposal and must contain at least the following information:

5.2.3.1 A complete narrative of the offeror's assessment of the work to be performed, the offeror's ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the offeror's understanding of the desired overall performance expectations.

5.2.3.2 A specific point-by-point response, in the order listed, to each requirement in the RFP as detailed in Sections 3 and 4. The response should identify each requirement being addressed as enumerated in the RFP.

5.2.3.3 A clear description of any options or alternatives proposed.

5.2.4 **Cost Proposal.** Cost will be evaluated independently from the technical proposal. Offerors may submit multiple cost proposals. All costs related to the provision of the required services must be included in each cost proposal offered.

See section 7.0 for more information related to the cost proposal.

6.0 PROPOSAL EVALUATION AND AWARD PROCESS

6.1 After determining that a proposal satisfies the mandatory requirements stated in the Request for Proposal, the evaluator(s) shall use subjective judgment in conducting a comparative assessment of the proposal by considering each of the following criteria listed in order of importance:

6.1.1 Specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements;

– –

6.1.2 Resources available to perform the work, including any specialized services, within the specified time limits for the project;

6.1.3 Record of past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration;

6.1.4 Familiarity with the project locale;

6.1.5 Cost proposal.

6.1.6 Availability to the project locale;

6.1.7 Proposed project management techniques;

6.1.8 Ability and proven history in handling special project constraints

6.2 Experience and reliability of the offeror's organization are considered subjectively in the evaluation process. Therefore, the offeror is advised to submit any information which documents successful and reliable experience in past performances, especially those performances related to the requirements of this RFP.

6.3 The qualifications of the personnel proposed by the offeror to perform the requirements of this RFP, whether from the offeror's organization or from a proposed subcontractor, will be subjectively evaluated. Therefore, the offeror should submit detailed information related to the experience and qualifications, including education and training, of proposed personnel.

6.4 The State reserves the right to reject any or all proposals, waive technicalities, and make award(s) as deemed to be in the best interest of the State of South Dakota.

6.5 **Award:** The requesting agency and the highest ranked offeror shall mutually discuss and refine the scope of services for the project and shall negotiate terms, including compensation and performance schedule.

6.5.1 If the agency and the highest ranked offeror are unable for any reason to negotiate a contract at a compensation level that is reasonable and fair to the agency, the agency shall, either orally or in writing, terminate negotiations with the contractor. The agency may then negotiate with the next highest ranked contractor.

6.5.2 The negotiation process may continue through successive offerors, according to agency ranking, until an agreement is reached or the agency terminates the contracting process.

7.0 COST PROPOSAL

The offeror shall enter their Cost Proposal on Attachment B and submit with their proposal.

Attachment A - Sample Contract

STATE OF SOUTH DAKOTA
DEPARTMENT OF SOCIAL SERVICES
HUMAN SERVICES CENTER

Consultant Contract
For Consultant Services
Between

State of South Dakota
Department of Social Services
Human Services Center
700 Governors Drive
Pierre, SD 57501-2291

Referred to as Consultant

Referred to as State

The State hereby enters into a contract (the "Agreement" hereinafter) for consultant services with the Consultant. While performing services hereunder, Consultant is an independent contractor and not an officer, agent, or employee of the State of South Dakota.

1. CONSULTANT'S South Dakota Vendor Number is .

2. PERIOD OF PERFORMANCE:
   A. This Agreement shall be effective as of and shall end on , unless sooner terminated pursuant to the terms hereof.

   B. Agreement is the result of request for proposal process, RFP #1695

3. PROVISIONS:
   A. The Purpose of this Consultant contract:
      1.

      2. Does this Agreement involve Protected Health Information (PHI)? YES (X) NO ( )
      If PHI is involved, a Business Associate Agreement must be attached and is fully incorporated herein as part of the Agreement (refer to Exhibit B) .

      3. The Consultant will use state equipment, supplies or facilities.

   B. The Consultant agrees to perform the following services (add an attachment if needed.):
      1.

   C. <u>The State agrees to:</u>
      1.

      2. Make payment for services upon satisfactory completion of services and receipt of bill. Payment will be in accordance with SDCL 5-26.

      3. Will the State pay Consultant expenses as a separate item?
      YES ( ) NO (X)
      If YES, expenses submitted will be reimbursed as identified in this Agreement.

D. Due to the subject matter of this Agreement, it requires the approval of the South Dakota Bureau of Information and Telecommunications ("BIT" hereinafter). The Consultant specifically agrees to the terms and conditions of the BIT supplementary contract clauses attached hereto as Exhibit A, the BIT Security Acknowledgement Form attached hereto as Exhibit C, the Information Technology Security Policy (ITSP) attached hereto as Exhibit D, and the BIT Permission to Scan attached hereto as Attachment C, which are collectively incorporated herein by reference and made a part hereof.

E. The TOTAL CONTRACT AMOUNT will not exceed **$.**

4. BILLING:
Consultant agrees to submit a bill for services within (30) days following the month in which services were provided. Consultant will prepare and submit a monthly bill for services. Consultant agrees to submit a final bill within 30 days of the Agreement end date to receive payment for completed services. If a final bill cannot be submitted in 30 days, then a written request for extension of time and explanation must be provided to the State.

5. TECHNICAL ASSISTANCE:
The State agrees to provide technical assistance regarding Department of Social Services rules, regulations and policies to the Consultant and to assist in the correction of problem areas identified by the State's monitoring activities.

6. LICENSING AND STANDARD COMPLIANCE:
The Consultant agrees to comply in full with all licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance in which the service and/or care is provided for the duration of this Agreement. The Consultant will maintain effective internal controls in managing the federal award. Liability resulting from noncompliance with licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance or through the Consultant's failure to ensure the safety of all individuals served is assumed entirely by the Consultant.

7. ASSURANCE REQUIREMENTS:
The Consultant agrees to abide by all applicable provisions of the following: Byrd Anti Lobbying Amendment (31 USC 1352), Executive orders 12549 and 12689 (Debarment and Suspension), Drug-Free Workplace, Executive Order 11246 Equal Employment Opportunity, Title VI of the Civil Rights Act of 1964, Title VIII of the Civil Rights Act of 1968, Section 504 of the Rehabilitation Act of 1973, Americans with Disabilities Act of 1990, Title IX of the Education Amendments of 1972, Drug Abuse Office and Treatment Act of 1972, Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970, Age Discrimination Act of 1975, Pro-Children Act of 1994, Hatch Act, Health Insurance Portability and Accountability Act (HIPAA) of 1996 as amended, Clean Air Act, Federal Water Pollution Control Act, Charitable Choice Provisions and Regulations, Equal Treatment for Faith-Based Religions at Title 28 Code of Federal Regulations Part 38, the Violence Against Women Reauthorization Act of 2013 and American Recovery and Reinvestment Act of 2009, as applicable; and any other nondiscrimination provision in the specific statute(s) under which application for Federal assistance is being made; and the requirements of any other nondiscrimination statute(s) which may apply to the award.

8. RETENTION AND INSPECTION OF RECORDS:
The Consultant agrees to maintain or supervise the maintenance of records necessary for the proper and efficient operation of the program, including records and documents regarding applications, determination of eligibility (when applicable), the provision of services, administrative costs, statistical, fiscal, other records, and information necessary for reporting and accountability required by the State. The Consultant shall retain such records for a period of six years from the date of submission of the final expenditure report. If such records are under pending audit, the Consultant agrees to hold such records for a longer period upon notification from the State. The State, through any authorized representative, will have access to and the right to examine and copy all records, books, papers or documents related to services rendered under this Agreement. State Proprietary Information retained in Consultant's secondary and backup systems will remain fully subject to the obligations of confidentiality stated herein until such information is erased or destroyed in accordance with Consultant's established record retention policies.

All payments to the Consultant by the State are subject to site review and audit as prescribed and carried out by the State. Any over payment of this Agreement shall be returned to the State within thirty days after written notification to the Consultant.

9. WORK PRODUCT:
Consultant hereby acknowledges and agrees that all reports, plans, specifications, technical data, drawings, software system programs and documentation, procedures, files, operating instructions and procedures, source code(s) and documentation, including those necessary to upgrade and maintain the software program, State Proprietary Information, as defined in the

Confidentiality of Information paragraph herein, state data, end user data, Protected Health Information as defined in 45 CFR 160.103, and all information contained therein provided to the State by the Consultant in connection with its performance of service under this Agreement shall belong to and is the property of the State and will not be used in any way by the Consultant without the written consent of the State.

Paper, reports, forms, software programs, source code(s) and other materials which are a part of the work under this Agreement will not be copyrighted without written approval of the State. In the unlikely event that any copyright does not fully belong to the State, the State nonetheless reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, and otherwise use, and to authorize others to use, any such work for government purposes.

Consultant agrees to return all information received from the State to State's custody upon the end of the term of this Agreement, unless otherwise agreed in a writing signed by both parties.

10. TERMINATION:
This Agreement may be terminated by either party hereto upon thirty (30) days written notice. In the event the Consultant breaches any of the terms or conditions hereof, this Agreement may be terminated by the State for cause at any time, with or without notice. Upon termination of this Agreement, all accounts and payments shall be processed according to financial arrangements set forth herein for services rendered to date of termination.

11. FUNDING:
This Agreement depends upon the continued availability of appropriated funds and expenditure authority from the Legislature for this purpose. If for any reason the Legislature fails to appropriate funds or grant expenditure authority, or funds become unavailable by operation of the law or federal funds reduction, this Agreement will be terminated by the State. Termination for any of these reasons is not a default by the State nor does it give rise to a claim against the State.

12. ASSIGNMENT AND AMENDMENTS:
This Agreement may not be assigned without the express prior written consent of the State. This Agreement may not be amended except in writing, which writing shall be expressly identified as a part hereof, and be signed by an authorized representative of each of the parties hereto.

13. CONTROLLING LAW:
This Agreement shall be governed by and construed in accordance with the laws of the State of South Dakota, without regard to any conflicts of law principles, decisional law, or statutory provision which would require or permit the application of another jurisdiction's substantive law. Venue for any lawsuit pertaining to or affecting this Agreement shall be resolved in the Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.

14. SUPERCESSION:
All prior discussions, communications and representations concerning the subject matter of this Agreement are superseded by the terms of this Agreement, and except as specifically provided herein, this Agreement constitutes the entire agreement with respect to the subject matter hereof.

15. IT STANDARDS:
Any software or hardware provided under this Agreement will comply with state standards which can be found at http://bit.sd.gov/standards/.

16. SEVERABILITY:
In the event that any provision of this Agreement shall be held unenforceable or invalid by any court of competent jurisdiction, such holding shall not invalidate or render unenforceable any other provision of this Agreement, which shall remain in full force and effect.

17. NOTICE:
Any notice or other communication required under this Agreement shall be in writing and sent to the address set forth above. Notices shall be given by and to the Division being contracted with on behalf of the State, and by the Consultant, or such authorized designees as either party may from time to time designate in writing. Notices or communications to or between the parties shall be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination shall be sent by registered or certified mail, or, if personally delivered, when received by such party.

18. SUBCONTRACTORS:
The Consultant may not use subcontractors to perform the services described herein without express prior written consent from the State. The State reserves the right to reject any person from the Agreement presenting insufficient skills or inappropriate behavior.

The Consultant will include provisions in its subcontracts requiring its subcontractors to comply with the applicable provisions of this Agreement, to indemnify the State, and to provide insurance coverage for the benefit of the State in a manner consistent with this Agreement. The Consultant will cause its subcontractors, agents, and employees to comply with applicable federal, state and local laws, regulations, ordinances, guidelines, permits and requirements and will adopt such review and inspection procedures as are necessary to assure such compliance. The State, at its option, may require the vetting of any subcontractors. The Consultant is required to assist in this process as needed.

19. STATE'S RIGHT TO REJECT:
The State reserves the right to reject any person or entity from performing the work or services contemplated by this Agreement, who present insufficient skills or inappropriate behavior.

20. HOLD HARMLESS:
The Consultant agrees to hold harmless and indemnify the State of South Dakota, its officers, agents and employees, from and against any and all actions, suits, damages, liability or other proceedings which may arise as the result of performing services hereunder. This section does not require the Consultant to be responsible for or defend against claims or damages arising solely from errors or omissions of the State, its officers, agents or employees.

21. INSURANCE:
Before beginning work under this Agreement, Consultant shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement. The Consultant, at all times during the term of this Agreement, shall obtain and maintain in force insurance coverage of the types and with the limits listed below. In the event a substantial change in insurance, issuance of a new policy, cancellation or nonrenewal of the policy, the Consultant agrees to provide immediate notice to the State and provide a new certificate of insurance showing continuous coverage in the amounts required. Consultant shall furnish copies of insurance policies if requested by the State.

A. Commercial General Liability Insurance:
Consultant shall maintain occurrence-based commercial general liability insurance or an equivalent form with a limit of not less than $1,000,000 for each occurrence. If such insurance contains a general aggregate limit, it shall apply separately to this Agreement or be no less than two times the occurrence limit.

B. Business Automobile Liability Insurance:
Consultant shall maintain business automobile liability insurance or an equivalent form with a limit of not less than $500,000 for each accident. Such insurance shall include coverage for owned, hired, and non-owned vehicles.

C. Worker's Compensation Insurance:
Consultant shall procure and maintain Workers' Compensation and employers' liability insurance as required by South Dakota law.

D. Professional Liability Insurance:
Consultant agrees to procure and maintain professional liability insurance with a limit not less than $1,000,000.

(Medical Health Professional shall maintain current general professional liability insurance with a limit of not less than one million dollars for each occurrence and three million dollars in the aggregate. Such insurance shall include South Dakota state employees as additional insureds in the event a claim, lawsuit, or other proceeding is filed against a state employee as a result of the services provided pursuant to this Agreement. If insurance provided by Medical Health Professional is provided on a claim made basis, then Medical Health Professional shall provide "tail" coverage for a period of five years after the termination of coverage.)

22. CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY, AND VOLUNTARY EXCLUSION:
Consultant certifies, by signing this Agreement, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by the federal government or any state or local government department or agency. Consultant further agrees that it will immediately notify the State if during the term of this Agreement either it or its principals become subject to debarment, suspension or ineligibility from participating in transactions by the federal government, or by any state or local government department or agency.

– –

23. CONFLICT OF INTEREST:
Consultant agrees to establish safeguards to prohibit employees or other persons from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain as contemplated by SDCL 5-18A-17 through 5-18A-17.6. Any potential conflict of interest must be disclosed in writing. In the event of a conflict of interest, the Consultant expressly agrees to be bound by the conflict resolution process set forth in SDCL 5-18A-17 through 5-18A-17.6.

24. CONFIDENTIALITY OF INFORMATION:
For the purpose of the sub-paragraph, "State Proprietary Information" shall include all information disclosed to the Consultant by the State. Consultant acknowledges that it shall have a duty to not disclose any State Proprietary Information to any third person for any reason without the express written permission of a State officer or employee with authority to authorize the disclosure. Consultant shall not: (i) disclose any State Proprietary Information to any third person unless otherwise specifically allowed under this Agreement; (ii) make any use of State Proprietary Information except to exercise rights and perform obligations under this Agreement; (iii) make State Proprietary Information available to any of its employees, officers, agents or consultants except those who have agreed to obligations of confidentiality at least as strict as those set out in this Agreement and who have a need to know such information. Consultant is held to the same standard of care in guarding State Proprietary Information as it applies to its own confidential or proprietary information and materials of a similar nature, and no less than holding State Proprietary Information in the strictest confidence. Consultant shall protect confidentiality of the State's information from the time of receipt to the time that such information is either returned to the State or destroyed to the extent that it cannot be recalled or reproduced. State Proprietary Information shall not include information that (i) was in the public domain at the time it was disclosed to Consultant; (ii) was known to Consultant without restriction at the time of disclosure from the State; (iii) that is disclosed with the prior written approval of State's officers or employees having authority to disclose such information; (iv) was independently developed by Consultant without the benefit or influence of the State's information; (v) becomes known to Consultant without restriction from a source not connected to the State of South Dakota. State's Proprietary Information shall include names, social security numbers, employer numbers, addresses and all other data about applicants, employers or other clients to whom the State provides services of any kind. Consultant understands that this information is confidential and protected under applicable State law at SDCL 1-27-1.5, modified by SDCL 1-27-1.6, SDCL 28-1-29, SDCL 28-1-32, and SDCL 28-1-68 as applicable federal regulation and agrees to immediately notify the State if the information is disclosure, either intentionally or inadvertently. The parties mutually agree that neither of them shall disclose the contents of the Agreement except as required by applicable law or as necessary to carry out the terms of the Agreement or to enforce that party's rights under this Agreement. Consultant acknowledges that the State and its agencies are public entities and thus are bound by South Dakota open meetings and open records laws. It is therefore not a breach of this Agreement for the State to take any action that the State reasonably believes is necessary to comply with the South Dakota open records or open meetings laws. If work assignments performed in the course of this Agreement require additional security requirements or clearance, the Consultant will be required to undergo investigation.

25. REPORTING PROVISION:
Consultant agrees to report to the State any event encountered in the course of performance of this Agreement which results in injury to any person or property, or which may otherwise subject Consultant, or the State of South Dakota or its officers, agents or employees to liability. Consultant shall report any such event to the State immediately upon discovery.

Consultant's obligation under this section shall only be to report the occurrence of any event to the State and to make any other report provided for by their duties or applicable law. Consultant's obligation to report shall not require disclosure of any information subject to privilege or confidentiality under law (e.g., attorney-client communications). Reporting to the State under this section shall not excuse or satisfy any obligation of Consultant to report any event to law enforcement or other entities under the requirements of any applicable law.

26. THE STATE OF SOUTH DAKOTA TECHNOLOGY OVERSIGHT

Pursuant to South Dakota Codified Law 1-33-44, the Bureau of Information and Telecommunications ("BIT") oversees the acquisition of office systems technology, software and services; telecommunication equipment, software and services; and data processing equipment, software, and services for departments, agencies, commissions, institutions and other units of state government. It is understood and agreed to by all parties that BIT, as the State's technology governing organization, has reviewed only the technology portion of this agreement. Before renewal of this Agreement BIT must review and approve the technology portion of this Agreement as still being current. BIT's evaluation will be based on changes in the IT security or regulatory requirements. Changes to the Agreement must be approved in writing by all parties before they go into effect and a renewal of this Agreement is possible. The most current version of the State's Information Technology Security Policy will also be provided to the Consultant with the understanding that the Consultant will adhere to the most current State IT security policies.

27. AUTHORIZED SIGNATURES:

In witness hereto, the parties signify their agreement by affixing their signatures hereto.

Consultant Signature		Date
Consultant Printed Name		
State – DSS Administrator HSC Kenneth Cole		Date
State - DSS Chief Financial Officer Laurie Mikkonen		Date
State – BIT Pat Snow (Interim Commissioner)		Date
State – DSS Deputy Secretary Amy Iversen-Pollreisz		Date

State Agency Coding:

CFDA #				
Company				
Account				
Center Req				
Center User				
Dollar Total				

DSS Program Contact Person _____

Phone _____

DSS Fiscal Contact Person Contract Accountant

Phone 605 773-3586

Consultant Program Contact Person _____

Phone _____

Consultant Program Email Address _____

Consultant Fiscal Contact Person _____

Phone _____

Consultant Fiscal Email Address _____

SDCL 1-24A-1 states that a copy of all consulting contracts shall be filed by the State agency with the State Auditor within five days after such contract is entered into and finally approved by the contracting parties. For further information about consulting contracts, see the State Auditor's policy handbook.

Exhibit A – Supplemental BIT Contract Clauses

The following contract clauses are provide by BIT in their role of overseeing the the acquisition of software and services for departments, agencies, commissions, institutions and other units of state government

1. THREAT NOTIFICATION:
   Upon becoming aware of a possible credible security threat with the Consultant's product(s) and or service(s) being used by the State, the Consultant or any subcontractor suppling product(s) or service(s) to the Consultant needed to fulfill the terms of this Agreement will notify the State within two (2) business days of any such threat. If the State requests, the Consultant will provide the State with information on the threat. A credible threat consists of the discovery of an exploit that a person considered an expert on Information Technology security believes could be used to breach one or more aspects of a system that is holding State data, or a product provided by the Consultant.

2. SECURITY INCIDENTS REGARDING PROTECTED HEALTH INFORMATION
   Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system as defined in 45 CFR 164.304. The Consultant shall alert the State Contact within twelve (12) hours of a Security Incident and provide daily updates to the BIT contact at their request. The Parties agree that this alert does not affect the Consultant's obligations under the Business Associate Agreement or the requirements of 45 CFR 164.410. The parties agree that, to the extent probes and reconnaissance scans common to the industry constitute a Security Incident, this Agreement constitutes notice by Consultant of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State shall be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Consultant's firewall, port scans, and unsuccessful log-on attempts, as long as such probes and reconnaissance scans do not result in a Security Incident as defined above. The State can require the Consultant to conduct a review or investigation within the scope and methodology determined by the State. At the State's discretion, the review or investigation may be performed by a third party at the Consultant's expense.

   Notwithstanding any other provision of this Agreement and in addition to any other remedies available to the State under law or equity, in the event the investigation or review determines that the consultant is responsible for the Security Incident, and where the State incurs any costs in the investigation, review or remediation of the Security Incident, the Consultant shall reimburse the State in full for all such costs. Costs include, but are not limited to, providing notification to regulatory agencies or other entities as required by law or contract. In the event the investigation or review determines that the consultant is responsible for the Security Incident, the Consultant shall also pay any and all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident, and all costs associated with the remediation of the Consultant's services and/or product(s).

3. REJECTION OR EJECTION OF CONSULTANT, AND CONSULTANT'S SUBCONTRACTORS, AGENTS, ASSIGNS AND/OR AFFILIATED ENTITIES EMPLOYEE(S)
   The State, at its option, may require the vetting of any of the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities. The Consultant is required to assist in this process as needed. The State reserves the right to reject any person from the project who the State believes would be detrimental to the project or is considered by the State to be a security risk.

   The State reserves the right to require the Consultant to remove from the project any person the State believes is detrimental to the project or is considered by the State to be a security risk. The State will provide the Consultant with notice of its determination, and the reasons removal is deemed necessary. If the State signifies that a potential security violation exists with respect to the request, the Consultant shall immediately remove the individual from the project.

4. SECURITY ACKNOWLEDGEMENT FORM

The Consultant will be required to sign the Security Acknowledgement form which is attached to this Agreement as Exhibit C. The signed Security Acknowledgement form must be submitted to the State and approved by the South Dakota Bureau of Information and Telecommunications and communicated to the Consultant by the State contact before work on the contract may begin. This form constitutes the agreement of Consultant to be responsible and liable for ensuring that the Consultant, Consultant's employee(s), and Subcontractor's, Agents, Assigns and or Affiliated Entities and all of their employee(s), participating in the work will abide by the terms of the Information Technology Security Policy-(ITSP) attached to this Agreement as Exhibit D. Failure to abide by the requirements of the ITSP or the Security Acknowledgement form can be considered a breach of this Agreement at the discretion of the State. It is also a breach of this Agreement, at the discretion of the State, if the Consultant does not sign another Security Acknowledgement form covering any employee(s) and any Subcontractor's, Agents, Assigns and or Affiliated Entities employee(s), any of whom are participating in the work covered by this Agreement, and who begin working under this Agreement after the project has begun. Any disciplining of the Consultant's, Consultant's employee(s) or Subcontractor's, Agents, Assigns and or Affiliated Entities employee(s) due to a failure to abide by the terms of the Security Acknowledgement Form will be done at the discretion of the Consultant or Subcontractor's, Agents, Assigns and or Affiliated Entities and in accordance with the Consultant's or Subcontractor's, Agents, Assigns and or Affiliated Entities personnel policies. Regardless of the actions taken by the Consultant and Subcontractor's, Agents, Assigns and or Affiliated Entities, the State shall retain the right to require at its discretion the removal of the employee(s) from the project covered by this agreement.

5. BACKGROUND CHECKS

The State requires all employee(s) of the Consultant, Subcontractors, Agents, Assigns and or Affiliated Entities who write or modify State owned software, alter hardware, configure software of state-owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas to undergo fingerprint-based background checks. These fingerprints will be used to check the criminal history records of both the State and the Federal Bureau of Investigation. These background checks must be performed by the State with support from the State's law enforcement resources. The State will supply the finger print cards and prescribe the procedure to be used to process the finger print cards. Project plans should allow two (2) to four (4) weeks to complete this process. If work assignments change after the initiation of the project covered by this agreement so that employee(s) of the Consultant, Subcontractor's, Agents, Assigns and or Affiliated Entities will be writing or modifying State owned software, altering hardware, configuring software of state owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas then, background checks must be performed on any employees who will complete any of the referenced tasks. The State reserves the right to require the Consultant to prohibit any employee, Subcontractors, Agents, Assigns and or Affiliated Entities from performing work under this Agreement whenever the State, in its sole discretion, believes that having a specific employee, subcontractor, agent assign or affiliated entity performing work under this Agreement is detrimental to the project or is considered by the State to be a security risk, based on the results of the background check. The State will provide the Consultant with notice of this determination.

6. PRODUCT INSTALLATION AND OPERATION

The State will install and operate the Consultant's product on the State's computing infrastructure. The State's installation process and operation of the product will follow current State standards which can be found at http://bit.sd.gov/standards/. It is the Consultant's responsibility to review these standards and alert the state if the costs enumerated in the agreement will change based on State standards. The State will not be responsible for added licensing or processing costs if the Consultant determines at a later date, that by following the standards in effect at the time of installation the State is or would be obligated to pay fines, additional rates, fees, license costs or charges of any type, additional charges of any type or character for Consultant's or a third party's intellectual property, or added support costs.

7. SECURITY

The Consultant shall take all actions necessary to protect State information from exploits, inappropriate alterations, access or release, and malicious attacks.

8. By signing this agreement, the Consultant warrants that:

A. All known security issues are resolved.

B. Assistance will be provided to the State by the Consultant in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. This investigation can include security scans made at the State's discretion.

C. State technology standards, policies, and best practices will be followed. State technology standards can be found at http://bit.sd.gov/standards/.

D. The Consultant will fully support and maintain the Consultant's application on platforms and code bases (including but not limited to: operating systems, hypervisors, web presentation layers, communication protocols, security products, report writers, and any other technologies on which the application depends) that are still being supported, maintained, and patched by the applicable third parties owning them. The Consultant may not withhold support from the State for this application nor charge the State additional fees as a result of the State moving the Consultant's application to a new release of third-party technology if:

i. The previous version of the third-party code base or platform is no longer being maintained, patched, and supported; and
ii. The new version to which the State moved the application is actively maintained, patched, and supported.

If there are multiple versions of the applicable code base or platform(s) supported by the third party in question, the Consultant may limit their support and maintenance to any one or all of the applicable third-party code bases or platforms.
If a code base or platform on which the Consultant's application depends is no longer supported, maintained, or patched by a qualified third party the Consultant commits to migrate its application from that code base and/or platform to one that is supported, maintained, and patched after the State has performed a risk assessment using industry standard tools and methods. Based on that assessment, the Consultant will fix or mitigate the risk based on the following schedule: high risk, within 7 days, medium risk within 14 days, low risk, within 30 days. Failure on the part of the Consultant to work in good faith with the State toward a timely move to supported, maintained, and patched technology will allow the State to cancel this Agreement without penalty.

9. LICENSE TO PERFORM SECURITY SCANNING

The Consultant will provide the State, at a time and for duration agreeable to both parties, access to the application and underlying hardware referenced in this Agreement for security scanning activities. Any scanning performed by the State will not be considered a violation of any licensure agreements the State has with the Consultant or the Consultant has with a third-party. Scanning by the State or any third-party acting for the State will not be considered reverse engineering. If the state security scanning efforts discover security issues, the State may collaborate, at the State's discretion, with the Consultant on remediation efforts. These remediation efforts will not be considered a violation of any licensure agreements the State has with the Consultant. The State will be indemnified and held harmless by the Consultant from all actions, lawsuits, damages (including all ordinary, incidental, consequential, and exemplary damages) or other proceedings that arise from security scanning, remediation efforts, and any after effects of security scanning or remediation. This indemnification includes all defense costs as well as reasonable attorneys' fees the State of South Dakota is required to pay in any such proceedings. The State will not be charged for any costs incurred by Consultant in these remediation efforts unless agreed to by the State in advance in writing. In the event of conflicting language this clause supersedes any other language in this or any other agreement made between the State and the Consultant.

10. SECURITY SCANNING

At the State's discretion, security scanning will be performed and or security settings put in place or altered during pre-production review for new or updated code. These scans and tests, can be time consuming and should be accounted for in project planning documents and schedules. Products not meeting the State's security and performance requirements will not be allowed into production until all issues are addressed to the State's satisfaction. The State urges the use of industry scanning/testing tools and recommends secure development methods are employed to avoid unexpected costs and project delays. Costs to produce and deliver secure and reliable applications are the responsibility of the Consultant producing or delivering an application to the State. Unless expressly indicated in writing, the State assumes all price estimates and bids are for the delivery and support of applications and systems that will pass security and performance testing.

11. MALICIOUS CODE

A. The Consultant warrants that the license software contains no code that does not support an application requirement.
B. The Consultant warrants that the license software contains no malicious code.
C. The Consultant warrants that the Consultant will not insert into the license software or any media on which the license software is delivered any malicious or intentionally destructive code.

D. The Consultant warrants that the Consultant will use commercially reasonable efforts consistent with industry standards to scan for and remove any malicious code from the licensed software before installation. In the event any malicious code is discovered in the licensed software delivered by the Consultant, the Consultant shall provide the State at no charge with a copy of the applicable licensed software that contains no malicious code or otherwise correct the affected portion of the services provided to the State. The remedies in this paragraph are in addition to other additional remedies available to the State.

12. DENIAL OF ACCESS OR REMOVAL OF AN APPLICATION AND OR HARDWARE FROM PRODUCTION
During the life of this Agreement the application and or hardware can be denied access to or removed from production at the State's discretion. The reasons for the denial of access or removal of the application and or hardware from the production system may include but not be limited to security, functionality, unsupported third-party technologies, or excessive resource consumption. Denial of access or removal of an application and or hardware also may be done if scanning shows that any updating or patching of the software and or hardware produces what the state determines are unacceptable results. The Consultant will be liable for additional work required to rectify issues concerning security, functionality, unsupported third-party technologies, and or excessive consumption of resources if it is for reasons of correcting security deficiencies or meeting the functional requirements originally agreed to for the application and or hardware. At the discretion of the State, contractual payments may be suspended while the application and or hardware is denied access to or removed from production. The reasons can be because of the Consultant's actions or inactions. Access to the production system to perform any remedying of the reasons for denial of access or removal of the software and hardware, and its updating and or patching will be made only with the State's prior approval. It is expected that the Consultant shall provide the State with proof of the safety and or effectiveness of the remedy, update or patch proposed before the State provides access to the production system. The State shall sign a non-disclosure agreement with the Consultant if revealing the update or patch will put the Consultant's intellectual property at risk. If the remedy, update or patch the Consultant proposes is unable to present software and or hardware that meets the State's requirements, as defined by the State, which may include but not limited to security, functionality, unsupported third party technologies, to the State's satisfaction within thirty (30) days of the denial of access to or removal from the production system then at the State's discretion the Agreement may be terminated.

13. MOVEMENT OF PRODUCT
The State operates a virtualized computing environment and retains the right to use industry standard hypervisor high availability, fail-over, and disaster recovery systems to move instances of the product(s) between the install sites defined with the Consultant within the provisions of resource and usage restrictions outlined elsewhere in the agreement. As part of normal operations, the State may also install the product on different computers or servers if the product is also removed from the previous computer or server within the provisions of resource and usage restrictions outlined elsewhere in the agreement. All such movement of product can be done by the State without any additional fees or charges by the Consultant.

14. USE OF PRODUCT ON VIRTUALIZED INFRASTRUCTURE AND CHANGES TO THAT INFRASTRUCTURE
The State operates a virtualized computing environment and uses software-based management and resource capping. The State retains the right to use and upgrade as deemed appropriate its hypervisor and operating system technology and related hardware without additional license fees or other charges provided the State assures the guest operating system(s) running within that hypervisor environment continue to present computing resources to the licensed product in a consistent manner. The computing resource allocations within the State's hypervisor software-based management controls for the guest operating system(s) executing the product shall be the only consideration in licensing compliance related to computing resource capacity.

15. LOAD BALANCING
The State routinely load balances across multiple servers, applications that run on the State's computing environment. The Consultant's product must be able to be load balanced across multiple servers. Any changes or modifications required to allow the Consultant's product to be load balanced so that it can operate on the State's computing environment will be at the Consultant's expense.

16. BACKUP COPIES
The State may make and keep backup copies of the licensed product without additional cost or obligation on the condition that:
A. The State maintains possession of the backup copies.
B. The backup copies are used only as bona fide backups.

17. USE OF ABSTRACTION TECHNOLOGIES

The Consultant's application must use abstraction technologies in all applications, that is the removal of the network control and forwarding functions that allows the network control to become directly programmable and the underlying infrastructure to be separated for applications and network services.

The Consultant warrants that hard-coded references will not be used in the application. Use of hard-coded references will result in a failure to pass pre-production testing or may cause the application to fail or be shut down at any time without warning and or be removed from production. Correcting the hardcoded references is the responsibility of the Consultant and will not be a project change chargeable to the State. If the use of hard-coded references is discovered after User Acceptance Testing the Consultant will correct the problem at no additional cost.

18. LICENSE AGREEMENTS

Consultant warrants that it has provided to the State and incorporated into this agreement all license agreements, End User License Agreements, and terms of use regarding its software or any software incorporated into its software before execution of this agreement. Failure to provide all such license agreements, End User License Agreements, and terms of use shall be a breach of this agreement at the option of the State. The parties agree that neither the State nor its end users shall be bound by the terms of any such agreements not timely provided pursuant to this paragraph and incorporated into this Agreement. Consultant agrees that it shall indemnify and hold the State harmless from any and all damages or other detriment, actions, lawsuits or other proceedings that arise from failure to provide all such license agreements, End User License Agreements, and terms of use or that arise from any failure to give the State notice of all such license agreements, End User License Agreements, and terms of use. Any changes to the terms of this Agreement or any additions or subtractions must first be agreed to by both parties in writing before they go into effect. This paragraph shall control and supersede the language of any such agreements to the contrary.

19. WEB AND MOBILE APPLICTIONS

The Consultant's application is required to;

A. have no code or services including web services included in or called by the application unless they provide direct, functional requirements that support the State's business goals for the application;
B. the documentation will be in grammatically complete text for each call and defined variables (Use no abbreviations and use complete sentences, for example.) sufficient for a native speaker of English with average programming skills to determine the meaning and/or intent of what is written without prior knowledge of the application.
C. have no code not required for the functioning of application;
D. have no "back doors", a back door being a means of accessing a computer program that bypasses security mechanisms, or other entries into the application other than those approved by the State;
E. permit no tracking of device user's activities without providing a clear notice to the device user and requiring the device user's active approval before the application captures tracking data;
F. have no connections to any service not required by the functional requirements of the application or defined in the project requirements documentation;
G. fully disclose in the "about" information that is the listing of version information and legal notices, of the connections made, permission(s) required, and the purpose of those connections and permission(s);
H. ask only for those permissions and access rights on the user's device that are required for the defined requirements of the Consultant's application;
I. access no data outside that which is defined in the "About" information for the Consultant's application;
J. Any application to be used on a mobile device must be password protected.

If the application does not adhere to the requirements given above or the Consultant has unacceptable disclosures, at the State's discretion, the Consultant will rectify the issues at no cost to the State.

20. APPLICATION PROGRAMMING INTERFACE

Consultant documentation on application programming interface must include a listing of all data types, functional specifications, a detailed explanation on how to use the Consultant's application programming interface and tutorials. The tutorials must include working sample code.

21. OFFSHORE SERVICES

The Consultant will not provide access to State data to any entity or person(s) located outside the continental United States that are not named in this agreement or without the written permission of the State.

22. MULTIFACTOR AUTHENTICATION

The Consultant must adhere to the requirements of level 3 authentication assurance for multifactor authentication as defined in NIST 800-63 when performing work under this contract where the Consultant potentially has access to legally protected State data or will be doing remote access to State systems. The Consultant must require that and all its Subcontractors, Agents. Assigns, and Affiliated Entities who potentially have access to legally protected State data also adhere to level 3 authentication assurance as defined in NIST 800-63, and Consultant shall be in breach of this contract if Consultant fails to so require.

23. CONSULTANT TRAINING REQUIREMENTS

The Consultant, Consultant's employee(s), and Consultant's Subcontractors, Agents, Assigns, Affiliated Entities and their employee(s), must successfully complete, at the time of hire and annually thereafter, a cyber-security training program. The training must include but is not limited to: i) Legal requirements for handling data, ii) Media sanitation, iii) Strong password protection, iv) Social engineering, or the psychological manipulation of persons into performing actions that are inconsistent with security practices or that cause the divulging of confidential information, v) Security incident response, and vi) Personal Health Information.

24. DATA SANITIZATION

At the end of the project covered by this Agreement the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities shall return the State's data and/or securely dispose of all State data in all forms, this can include State data on media such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. This State data must be permanently deleted by either purging the data or destroying the medium on which the State data is found according to the methods given in the most current version of NIST 800-88. Certificates of Sanitization for Offsite Data (See bit.sd.gov/vendor/default.aspx for copy of certificate) must be completed by the Consultant and given to the State Contact. The State will review the completed Certificates of Sanitization for Offsite Data. If the State is not satisfied by the data sanitization then the Consultant will use a process and procedure that does satisfy the State.

25. THIRD PARTY HOSTING

If the Consultant has the State's data hosted by another party the Consultant must provide the State, the name of this party. The Consultant must provide the State with contact information for this third party and the location of their data center(s). The Consultant must receive from the third party written assurances that the state's data will reside in the continental United States at all times and provide these written assurances to the State. This restriction includes the data being viewed or accessed by the third-party's employees or contractors. If during the term of this agreement the consultant changes from the Consultant hosting the data to a third-party hosting the data or changes third-party hosting provider, the Consultant will provide the State with one hundred and eighty (180) days' advance notice of this change and at that time provide the state with the information required above.

26. SECURING OF DATA

All facilities used to store and process State's data will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Consultant's own data of a similar type, and in no event less than commercially reasonable in view of the type and nature of the data involved. Without limiting the foregoing, the Consultant warrants that all State's data will be encrypted in transmission (including via web interface) and storage at no less than AES256 level encryption with SHA256 or SHA2 hashing.

27. SECURITY PROCESSES

The Consultant shall disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Consultant. For example: virus checking and port sniffing.

28. PASSWORD PROTECTION

_ _ The website(s) and or service(s) that will be hosted by the Consultant for the State will be password protected. If the Consultant provides the user with a preset or default password that password cannot include any Personally Identifiable Information, data protected under the Family Educational Rights and Privacy Act, Personal Heath Information, Federal Tax Information or any information defined under state statute as confidential Information or fragment thereof.

29. MOVEMENT OF PROTECTED STATE DATA

Any State data that is protected by Federal or State statute or requirements or by industry standards must be kept secure. When protected State data is moved to any of the Consultant's production or non-production systems, security must be maintained. The Consultant will ensure that that data will at least have the same level of security as it had on the State's environment. The State's security policies can be found in the Information Technology Security Policies (ITSP).

Exhibit B – Business Associate Agreement

STATE OF SOUTH DAKOTA
DEPARTMENT OF SOCIAL SERVICES

Business Associate Agreement

1. Definitions

General definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean the Provider, Consultant or entity contracting with the State of South Dakota as set forth more fully in the Agreement this Business Associate Agreement is attached.

(b) CFR. "CFR" shall mean the Code of Federal Regulations.

(c) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean South Dakota Department of Social Services.

(d) Designated Record Set. "Designated Record Set" shall have the meaning given to such term in 45 CFR 164.501.

(f) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164 (Subparts A, C, D and E). More specifically, the "Privacy Rule" shall mean the regulations codified at 45 CFR Part 160 and Part 164 (Subparts A and E), and the "Security Rule" shall mean the regulations codified at 45 CFR Part 160 and Part 164 (Subparts A and C).

(g) Protected Health Information. "Protected Health Information" or "PHI" shall mean the term as defined in 45 C.F.R. §160.103, and is limited to the Protected Health Information received from, or received or created on behalf of Covered Entity by Business Associate pursuant to performance of the Services under the Agreement.

2. Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not Use or Disclose Protected Health Information other than as permitted or required by the Agreement or as Required by Law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic Protected Health Information, to prevent Use or Disclosure of Protected Health Information other than as provided for by the Agreement;

(c) Report to covered entity any Use or Disclosure of Protected Health Information not provided for by the Agreement of which it becomes aware, including Breaches of Unsecured Protected Health Information as required at 45 CFR 164.410, and any Security Incident of which it becomes aware within five (5) business days of receiving knowledge of such Use, Disclosure, Breach, or Security Incident;

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any Subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Make available Protected Health Information in a designated record set to the covered entity as necessary to satisfy covered entity's obligations under 45 CFR 164.524. Business associate shall cooperate with covered entity to fulfill all requests by Individuals for access to the Individual's Protected Health Information that are approved by covered entity. If business associate receives a request from an Individual for access to Protected Health Information, business associate shall forward such request to covered entity within ten (10) business days. Covered entity shall be solely responsible for determining the scope of Protected Health Information and Designated Record Set with respect to each request by an Individual for access to Protected Health Information;

(f) Make any amendment(s) to Protected Health Information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526. Within ten (10) business days following any such amendment or other measure, business associate shall provide written notice to covered entity confirming that business associate has made such amendments or other measures and containing any such information as may be necessary for covered entity to provide adequate notice to the Individual in accordance with 45 CFR 164.526. Should business associate receive requests to amend Protected Health Information from an Individual, Business associate shall cooperate with covered entity to fulfill all requests by Individuals for such amendments to the Individual's Protected Health Information that are approved by covered entity. If business associate receives a request from an Individual to amend Protected Health Information, business associate shall forward such request to covered entity within ten (10) business days. Covered entity shall be solely responsible for determining whether to amend any Protected Health Information with respect to each request by an Individual for access to Protected Health Information;

(g) Maintain and make available the information required to provide an accounting of Disclosures to the covered entities necessary to satisfy covered entity's obligations under 45 CFR 164.528. Business associate shall cooperate with covered entity to fulfill all requests by Individuals for access to an accounting of Disclosures that are approved by covered entity. If business associate receives a request from an Individual for an accounting of Disclosures, business associate shall immediately forward such request to covered entity. Covered entity shall be solely responsible for determining whether to release any account of Disclosures;

(h) To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the covered entity and / or the Secretary of the United States Department of Health and Human Services for purposes of determining compliance with the HIPAA Rules.

3. Permitted Uses and Disclosures by Business Associate

(a) Except as otherwise limited by this Agreement, Business Associate may make any uses and Disclosures of Protected Health Information necessary to perform its services to Covered Entity and otherwise meet its obligations under this Agreement, if such Use or Disclosure would not violate the Privacy Rule if done by the covered entity. All other Uses or Disclosure by Business Associate not authorized by this Agreement or by specific instruction of Covered Entity are prohibited.

(b) The business associate is authorized to use Protected Health Information if the business associate de-identifies the information in accordance with 45 CFR 164.514(a)-(c). In order to de-identify any information, Business Associate must remove all information identifying the Individual including, but not limited to, the following: names, geographic subdivisions smaller than a state, all dates related to an Individual, all ages over the age of 89 (except such ages may be aggregated into a single category of age 90 or older), telephone numbers, fax numbers, electronic mail (email) addresses, medical record numbers, account numbers, certificate/ license numbers, vehicle identifiers and serial numbers (including license plate numbers, device identifiers and serial numbers), web universal resource locators (URLs), internet protocol (IP) address number, biometric identifiers (including finger and voice prints), full face photographic images (and any comparable images), any other unique identifying number, and any other characteristic or code.

(c) Business associate may Use or Disclose Protected Health Information as Required by Law.

(d) Business associate agrees to make Uses and Disclosures and requests for Protected Health Information consistent with covered entity's Minimum Necessary policies and procedures.

(e) Business associate may not Use or Disclose Protected Health Information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity except for the specific Uses and Disclosures set forth in (f) and (g).

(f) Business associate may Disclose Protected Health Information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the Disclosures are Required by Law.

(g) Business associate may provide Data Aggregation services relating to the Health Care Operations of the covered entity.

4. Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) Covered entity shall notify business associate of any limitation(s) in the Notice of Privacy Practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's Use or Disclosure of Protected Health Information.

(b) Covered entity shall notify business associate of any changes in, or revocation of, the permission by an Individual to Use or Disclose his or her Protected Health Information, to the extent that such changes may affect business associate's Use or Disclosure of Protected Health Information.

(c) Covered entity shall notify business associate of any restriction on the Use or Disclosure of Protected Health Information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's Use or Disclosure of Protected Health Information.

5. Term and Termination

(a) Term. The Term of this Agreement shall be effective as of and shall terminate on the dates set forth in the primary Agreement this Business Associate Agreement is attached to or on the date the primary Agreement terminates, whichever is sooner.

(b) Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement.

(c) Obligations of Business Associate Upon Termination.

1. Except as provided in paragraph (2) of this section, upon termination of this agreement for any reason, business associate shall return or destroy all Protected Health Information received from, or created or received by business associate on behalf of covered entity. This provision shall apply to Protected Health Information that is in the possession of Subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

2. In the event that business associate determines that returning or destroying the Protected Health Information is infeasible, business associate shall provide to covered entity, within ten (10) business days, notification of the conditions that make return or destruction infeasible. Upon such determination, business associate shall extend the protections of this agreement to such Protected Health Information and limit further Uses and Disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as business associate maintains such Protected Health Information.

(d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

6. Miscellaneous

(a) Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

(d) Conflicts. In the event of a conflict in between the terms of this Business Associate Agreement and the Agreement to which it is attached, the terms of this Business Associate Agreement shall prevail to the extent such an interpretation ensures compliance with the HIPAA Rules.

Exhibit C – Security Acknowledgement

All BIT employees and State contractors must sign; **Agreement to Comply with BIT Information Technology Security Policy (the "Policy").** Users are responsible for compliance to all information security policies and procedures. *By signature below, the employee or contractor hereby acknowledges and agrees to the following:*

1. Employee is a State of South Dakota employee or contractor that uses non-public State of South Dakota technology infrastructure or information;
2. Employee or contractor will protect technology assets of the State from unauthorized activities including disclosure, modification, deletion, and usage;
3. Employee or contractor agrees to follow state and federal regulations in regards to confidentiality and handling of data;
4. Employee or contractor has read and agrees to abide by the Policy;
5. Employee or contractor consents to discuss with a supervisor / State contact regarding Policy violations;
6. Employee or contractor shall abide by the policies described as a condition of continued employment / service;
7. Employee or contractor understands that any individual found to violate the Policy is subject to disciplinary action, including but not limited to, privilege revocation, employment termination or financial reimbursement to the State;
8. Access to the technology infrastructure of the State is a privilege which may be changed or revoked at the discretion of BIT management;
9. Access to the technology infrastructure of the State automatically terminates upon departure from the State of South Dakota employment or contract termination;
10. Employee or contractor shall promptly report violations of security policies to a BIT manager or State Contact and BIT Help Desk (605.773.4357);
11. The Policy may be amended from time to time. The State of South Dakota recommends employees and contractors for the State to regularly review the appropriate Policy and annual amendments.
    Information Technology Security Policy – BIT: http://intranet.bit.sd.gov/policies/
    Information Technology Security Policy – CLIENT: http://intranet.bit.sd.gov/policies/
    Information Technology Security Policy – CONTRACTOR: http://bit.sd.gov/vendor/default.aspx

Acknowledgement: State of South Dakota Information Technology Security Policy

Contractor: If the individual is signing for their entire company by signing this form the individual affirms that they have the authority to commit their entire organization and all its employees to follow the terms of this agreement.

_____	_____	_____	_____
Employee or Contractor signature	Date	BIT Manager or Contact	Date

_____

Employee or Contractor name and Company name in block capital letters

– –

Exhibit D - BIT Information Technology Security Policy (ITSP)

Beginning on next page

Information Technology Security Policy

ctor Version 4.0

19

General-Information Technology Security Policy-Introduction 7
1.1.4.1. General 13
1.1.4.2. Chief Information Security Officer 13
1.1.4.3. Security Infrastructure Team (SIT) 13
1.1.4.4. Security Operations Team (SOT) 14
1.1.4.5. BIT Executive Working Group on Cyber Security 14
Administrative -I/T Asset Protection-Background Checks 14
10.1.4.1. Background Checks 15
10.1.4.2. Disqualifying Criteria 15
10.1.4.3. Noncriminal Agency Coordinator (NAC) 16
10.1.4.4. Local Agency Security Officer (LASO) 16
10.1.4.5. Background Check Interpretation 16
10.1.4.6. Not Guilty Presumption 16
10.1.4.7. Background Check Information Challenge 16
10.1.4.8. Corrective Action 17
10.1.4.9. Training 17
10.1.4.10. Emailing Background Check Information 17
Administrative -I/T Asset Protection-Confidentiality 17
10.3.4.1. Confidentiality Agreement 18
10.3.4.2. Security Acknowledgement and Access 18
Mainframe-Mainframe Security-Mainframe Accounts 18
210.3.4.1. Unique Account Requirement 19
210.3.4.2. Requests for Mainframe User IDs 19
210.3.4.3. Responsibility for Mainframe UserIDs and Passwords 19
Mainframe-Mainframe Security-Mainframe Accounts 19
210.4.4.1. Mainframe User ID Revocation 20
Mainframe-Mainframe Security-Mainframe Access 20
210.25.4.1. Mainframe Access 21
Server-Server Security-Server Maintenance and Administration 21
220.1.4.1. Visibility of Server and Framework Patching Status 21
Server-Server Security-File Transfer Protocol 22
220.7.4.1. Use of File Transfer Protocol Server 22
Server-Server Security-Assurance HIPAA Regulations are Met 22
220.10.4.1. The Data User is Responsible for Adhering to HIPAA Regulations 23
Data Center General-Data Center Security-Cloud Based Services and System Information 23
230.9.4.1. Responsibility for Cloud Based Services and Systems 24
Data Center General-Secure Information Technology Acquisition Policy-Secure Information

Technology Acquisition Policy 24
230.10.4.1. Hardware Maintenance Agreements 25
Data Center General-Data Center Security-Federal Tax Information 25
230.11.4.1. Federal Tax Information Returns and Return Information 26
230.11.4.2. What is Not Federal Tax Information 26
230.11.4.3. Safeguarding Federal Tax Information 26
230.11.4.4. Emailing Federal Tax Information 26
Data Center General-Procedural-Physical Access - Proximity Cards 26
230.58.4.1. Proximity Card for Non-BIT Employee Access 27
Data Center General-Data Center Security-Accounts Access Control and Authorization 27
230.67.4.1. Individual Access Authorization 28
230.67.4.2. Least Privilege 28
230.67.4.3. Password Requirements 28
230.67.4.4. Individual Access Termination 29
Data Center General-Payment Card Industry Data Security-Payment Card Industry Data Security Standard 29
230.72.4.1. Payment Card Industry Data Security Standard Requirements 30
Data Center General-Secure Information Technology Acquisition Policy-Secure Information Technology Acquisition Policy 30
230.73.4.1. Acquisition of Services Involving HIPAA Data 31
230.73.4.2. Security Scanning Requirements 31
230.73.4.3. Hardware Maintenance Agreements 31
Data Center General-Use of Production Data-Use of Production Data in a Non-Production Environment 31
230.74.4.1. Use of Production Data in a Non-Production Environment 32
230.74.4.2. Purging of Data 33
230.74.4.3. Compliance 33
Data Center General -Security Impacts-Data Classification 34
230.75.4.1. Data Classification System 34
230.75.4.2. Classification of Data Produced under Contract 35
230.75.4.3. Data Classification Responsibilities 35
Data Center General-Access to Confidential Data-Multi-Factor Authentication 36
230.76.4.1. Usage of Multi-Factor Authentication (MFA) 36
230.76.4.2. MFA Tokens 37
Data Center General-Approved Disposal of State Data-Media Sanitization 37
230.77.4.1. Sanitization of Media in a Contractor's Control 37
Data Center General-Transfer of Data-Secure Transfer of Data 38

230.78.4.1. Use of Secure File Transfer Protocol 39
Development-Application Security-Federal Tax Information 39
401.1.4.1. Allocation of Resources and Life Cycle Support 40
401.1.4.2. Information System Security Documentation 40
401.1.4.3. Software Usage Restrictions and User Installed Software 40
401.1.4.4. Developer Configuration Management 40
Development-Application Security-Security Assessments 40
401.3.4.1. Security Assessment 41
401.3.4.2. Assessment Report 41
401.3.4.3. Annual Review 41
Development-Application Security-Data Encryption 42
401.5.4.1. Data Encryption 42
401.5.4.2. Hashing Values 42
401.5.4.3. Tools 42
401.5.4.4. Compliance Measurements 42
401.5.4.5. Exceptions 43
401.5.4.6. Non-Compliance 43
Development-Application Security-Authentication and Authorization 43
401.7.4.1. User Authentication and Authorization 43
401.7.4.2. Password Requirements 44
401.7.4.3. Invalid Login Attempts for projects using Federal Tax Information 44
401.7.4.4. reCAPTCHA 44
401.7.4.5. Tools 44
401.7.4.6. Compliance Measurements 44
401.7.4.7. Exceptions 44
401.7.4.8. Non-Compliance 44
Network-Service-Access Control 45
610.1.4.1. System Access Expectations 45
610.1.4.2. Contractor Access 46
610.1.4.3. Modems 46
610.1.4.4. Remote Access 46
610.1.4.5. Inspection and Review 47
610.1.4.6. Department of Social Services 47
Network-Concept-Security Domain Zones 47
610.3.4.1. Intranet 48

610.3.4.2. DMZ 48
610.3.4.3. Extranet 48
Network-Concept-Network Integrity 48
610.9.4.1. Responsibilities 49
610.9.4.2. Management 49
610.9.4.3. Disabling Critical Components of Network Security Infrastructure 49
610.9.4.4. Technical Asset or Contractor Connections 49
610.9.4.5. Local Area Network 49
610.9.4.6. Wide Area Network 49
610.9.4.7. Physical Controls 49
Network-Communication-Internet 50
610.11.4.1. Multiple Connections 50
610.11.4.2. Interfaces 50
610.11.4.3. Security 50
610.11.4.4. Responsibilities 51
610.11.4.5. IPv4/IPv6 and Device Names 51
Security-Network Discovery-Probing-Exploiting 51
620.1.4.1. Limiting Tool Functionality 52
620.1.4.2. Exploiting Security Controls of Information Systems 52
620.1.4.3. Cracking Application or Passwords 52
620.1.4.4. Exemptions 52
Security-Content Control-Internet Filtering 52
620.5.4.1. Exemptions 53
620.5.4.2. Appropriate Use of Administrator Access 53
620.5.4.3. DDN Content Filtering 54
620.5.4.4. DDN Intranet Content Filtering 54
620.5.4.5. Filter Exemption Requests 54
TERMS 55
ACRONYMS 63

ITSP Change Log

Policy Number	Policy Title	New	Revised	Deleted
220.1.4.3	Visibility of Server and Framework patching Status	03.01.2019		
230.74.4.1	Use of Production Data in a Non-Production Environment	03.01.2019		
230.67.4.6	Password Requirements	03.01.2019		
230.67.4.11	Non-Expiring Passwords	03.01.2019		
230.75.4.1	Data Classification System		03.01.2019	
230.76	Multi-Factor Authentication		03.01.2019	
230.77	Media Sanitization	03.01.2019		
230.78	Use of SFTP	03.01.2019		
401.5	Data Encryption		03.01.2019	
401.7	Authentication and Authorization		03.01.2019	
610.1	Access Control		03.01.2019	
10.1.4.1	Background Checks		06.01.2018	
230.67.4.2	User Privilege Capabilities		06.01.2018	
230.74	Use of Production Data in a Non-Production Environment		06.01.2018	
210.20	Disposition of Mainframe Output and Documentation		09.26.2018	
230.9	Cloud Based Services and System Information		09.26.2018	
230.67	Accounts Access Control and Authorization		09.26.2018	
230.72	Payment Card Industry Data Security Standard			09.26.2018
230.74	Use of Production Data in a Non-Production Environment		09.26.2018	
230.75	Data Classification			09.26.2018

Staff Augmentation Contractors must follow the BIT Version of the ITSP. Any policy that was included in the Contractor Version only for Staff Augmentation Contractors has been removed from this version. 03.01.2019

General-Information Technology Security Policy-Introduction

1.1.1. Overview

This Information Technology (IT) Security Policy has been developed by the Bureau of Information & Telecommunications (BIT) of the State of South Dakota. The Information Technology Security Policy provides guidance regarding cyber security policies of the State relevant to the IT goals, beliefs, ethics, and responsibilities. Specific procedures that State employees and contractors must follow to comply with the security objectives are identified.

The objective of the Information Technology Security Policy is to provide a comprehensive set of cyber security policies detailing the acceptable practices for use of State of South Dakota IT resources. The security policies and procedures set forth are to accomplish the following:

- Assure proper implementation of security controls within the BIT environment.
- Assure government data is protected regardless of hosting location.
- Demonstrate commitment and support to the implementation of security measures by BIT and Executive management.
- Avoid litigation by documenting acceptable use of State IT resources.
- Achieve consistent and complete security across the diverse technology infrastructure of the State and hosted State data.

The Information Technology Security Policy, when combined with individual, specific security procedures, provides a comprehensive approach to security planning and execution to ensure that State managed assets are afforded appropriate levels of protection against destruction; loss; unauthorized access, change, or use; and disruption or denial of service.

BIT is responsible for maintaining and updating this policy. An updated version of the Information Technology Security Policy will be posted to the Intranet annually the first of March. The Commissioner of BIT or the Chief Information Security Officer can authorize an out of cycle or special edition to be released.

Information Technology Security is based on three principles:

- Confidentiality
- Integrity
- Availability

Confidentiality - ensuring that only permitted individuals are able to view information pertinent to apply defined responsibilities.

Integrity - the information is accurate because nothing has been changed or altered.

Availability - the technology infrastructure and services built upon that infrastructure are not intentionally disrupted and are available for use by the clientele in a dependable and reliable manner.

Each individual policy defined herein falls within one or more of these guiding principles.

Information Technology security requires on-going vigilance, and employees should understand the importance of cyber security in the protection of State data and technology resources along with the personal/home computing/data assets of every individual. Guardianship of State data, infrastructure, and applications is a critical

priority for BIT. The effort is complicated by the balance needed between usability/service and meaningful protection.

BIT Mission Statement

The Bureau of Information and Telecommunications (BIT) strives to partner and collaborate with clients in support of their missions through innovative information technology consulting, systems, and solutions.

Vision

Through our highly motivated staff - we will be a Leader and valued partner in providing technology solutions, services, and support that directly contribute to the success of our clients.

Goals:

Provide a Reliable, Secure and Modern Infrastructure.

Provide a well-designed and architected secure computing and communications environment to ensure optimal service delivery to business. Architecture and process will be optimized to support agile and reliable computing and communication services.

Technology assets must be high performing and dependable to ensure services are available whenever needed. Centralization, standardization, and collaboration are vital to efficiently leverage investments. To maintain public trust, we must secure data and technology assets through leading security tools, policies, and practices.

Deliver Valuable Services at Economical Costs.

Develop innovative and cost-effective solutions through collaboration, cooperation, and in partnership with our clients. The solution sets include developing customized business solutions, efficient project management services, and productive relationships with clients.

Regarding our citizens interacting with their government: "People should be online, not waiting in line. "

Build and Retain a Highly Skilled Workforce.

Improve the effectiveness, productivity, and satisfaction of employees in order to attract (and retain) a highly qualified workforce to foster individual innovation and professional growth. Appropriate training and tools will be provided to enhance and improve career skills in the workforce.

Information technology systems are critical, valuable assets. Policies relating to the valuable assets are important to ensure that all entities receive adequate information to enable the department, office, and agency to provide a basic level of protection to the technology systems.

Security is not accomplished at a single point or by a single individual! (Or in a single point in time!)

Instead of relying on one person or a firewall or anti-virus software or some other single piece of hardware or software, a series of assets and entities together build a safe computing environment. Technically, a layered approach is taken to accomplish security within the State which is called the Information Technology (IT) Security Model. A foundation is established; additional layers may build on the previous layer or may also act independently to provide separate security measures. Each point of accessibility into the wired and wireless network creates security concerns. Security is not limited to technology. A critical portion of cyber security is the human aspect.

Information Technology Security Model

The different technology layers of the Information Technology Security Model create opportunities for implementing security:

- User Education involves the training of employees to ensure that proper awareness is brought to the topic of security including steps to take when incidents occur that are outside of the scope of the daily work routine.
- Physical Access is taking appropriate steps to physically safeguard technical equipment such as outlining procedures to prevent workstations from being stolen which can include limiting access to a particular room or locking up the device in a cabinet.
- Network Access includes protecting the State Network from unauthorized access via internal methods and from outside our physical offices. Because technology can be manipulated by individuals or workstations to create a detrimental outcome, safeguards must be implemented to prevent, thwart, and repel workstation attacks from inside State Government and the Internet; access protection is not limited to workstations, it includes smartphones, Internet of Thing devices, environmental controls, and network - network connectivity.
- Workstation Platform means taking advantage of the inherent feature sets of workstation platforms. For example, user id and password capabilities must be used as intended within the workstation platform.
- Cyber Strength Evaluation of business software must apply across in-house developed and third party built or supplied software applications. New applications must be tested before being placed into service and existing applications must be re-evaluated on a regular basis.
- Cyber security language is incorporated within all information technology (I/T) requests for proposals and I/T contracts.
- Information System security entails designing the necessary security features and permissions to ensure that only legitimized staff have proper resource access. The design must consider areas such as viewers of departmental data to individuals that can add data or update records.
- Data security is the protection of the asset; often referred to as the "money in the vault". Insuring that data is only accessible by permitted applications and personnel is the core of the security model. The data could be credit card numbers, social security numbers, health records, or financial information.

Partners

The IT Security model goal is to ensure that the hardware, software, and data technology assets of the State are protected in a reasonable and prudent manner. Planning, cooperation, and assistance from many different entities is required to meet the goal. The State has various partners in cyber security efforts. BIT must continue to evolve relationships with:

- State government of South Dakota branches departments, and constitutional offices
- Internet Service Providers
- Multi-State Information and Sharing Center (MS ISAC)
- Department of Homeland Security
- State Fusion Center
- Federal Bureau of Investigation (FBI) - InfraGard program
- National Association of State Technology Directors (NASTD)
- National Association of Chief Information Officers (NASCIO)
- SysAdmin, Audit, Networking, and Security (SANS)
- Microsoft, Inc.
- Symantec, Inc.
- US CERT
- A variety of hardware and software contractors.

All of these organizations contribute to the development of cyber security information sharing, policies, procedures, and metrics. In return, specific reporting is distributed amongst the partners.

Roles and Responsibilities

In the application of information technology, BIT is responsible for providing leadership, policy, and technical support to all agencies of the Executive branch of the State of South Dakota. Also, various levels of support are provided to the Judicial branch, constitutional offices of government, K-12 education, and higher education. In addition to data center operations and related end user and customer support services, the broad statement of roles and responsibilities encompasses major information resource functions such as development, delivery, administration of voice, data, and video, applications - to include services, software, hardware selection, installation, and support.

Individual roles and responsibilities are defined herein; the following responsibilities are shared by all:

- Participate in information security awareness program activities.
- Read, understand, and follow the policies defined in the **Information Technology Security Policy**.
- Report all violations, security incidents, suspected, and/or attempted security incidents to BIT. BIT

Commissioner:

The Commissioner of the Bureau of Information & Telecommunications for the State of South Dakota is responsible for ensuring that:

- Reasonable security measures are taken to protect sensitive files and information.
- Enforceable security rules are created and disseminated.
- System resources are managed and monitored to ensure prudent and legitimate usage.
- Alleged security violations are addressed, and problems are investigated.
- Designated individuals are responsible for design, configuration, and support of technology resources.

Employees and Contractors are responsible for:

- Taking the time to read, understand, and ask questions if necessary to clarify the policies defined herein.
- Fully adhering to these policies defined herein.
- Agreeing that use of State technologies which includes equipment, applications, and resources are for work-related purposes.
- Applying recommended password policies.
- Safeguarding sensitive information whether employee / contractor is in the office or traveling for the State.
- Reporting any unusual requests for information or obvious security incidents to the BIT Help Desk.
- Immediately reporting loss of any State technology devices or data.
- Understanding that everyone is a potential target of nefarious individuals seeking 'social engineering' information to be used for illegally accessing State of South Dakota systems and technologies; Hence, be aware that any information provided to outside entities can be dangerous.
- Protecting information technology assets by following policies and procedures.
- Ensuring each individual is authorized to use a given technical asset.
- Understanding and complying with the policies, procedures, and laws related to conditions of use authorizing access to BIT systems and data.
- Not subverting or attempting to subvert security measures.

Department, Office, Division, or Group Managers are responsible for:

- Creating, disseminating, and enforcing conditions of use for technology and applications in areas of

responsibility.

- Responding to concerns regarding alleged or real violations of this policy.
- Ensuring that their employees understand security responsibilities.
- Monitoring the use of South Dakota technology resources by observing usage.

- Determining the access requirements of staff, and ensuring completion of the appropriate forms, including all required authorizations for the application(s) requested by insuring only legitimate staff have access to the set of functions needed to perform defined tasks.
- Communicating terminations and status changes of individuals immediately to the Bureau of Human Resources (BHR) through BHR-defined procedures so that BIT is notified to ensure proper deletion or revision of user access is performed.
- Ensuring a secure physical environment for the staff use of State equipment, information systems, and data.

Bureau of Information & Telecommunications (BIT) is responsible for:

- Taking reasonable action to assure the authorized use and security of data, networks, applications, and communications amongst these technologies.
- Promptly responding to client questions on details relating to appropriate use of technical resources.
- Providing advice regarding the development of conditions of use or authorized use and procedures through work order requests.
- Ensuring that investigations into any alleged personal workstation or network security compromises, incidents, or problems are conducted.
- Ensuring that appropriate security controls are enabled and are being followed in coordination with BIT staff that are responsible for security administration.
- Verifying and authorizing individuals for an appropriate level of access to only the resources required to perform one's responsibilities.
- Overseeing that an individual has the necessary security authorizations in order for the person to perform assigned duties or tasks.
- Cooperating with appropriate departments, branches, agencies, and law enforcement officials in the course of investigation of alleged violations of policy or law.
- Overseeing the administration of BIT employee and contractor access to BIT facilities.
- Coordinating disaster recovery and testing exercises.

Data Owners

All data files, information, and applications belong to the State. Authorized users or agents of the data are the State of South Dakota departments, agencies, and offices. Files in central systems belong to the account owner. Data owners are responsible for:

- Tracking the data owned/managed by the agency and agency staff.
- Providing BIT notification within 24 hours of any notices regarding federal/state/or industry audits related to any aspects of an agency data, electronic communications, or data processing.
- Working with BIT to ensure access to the data and application(s) is limited to individuals with a legitimate need for the resource access.
- Ensuring that security measures and standards are implemented and enforced in a method consistent with BIT security policies and procedures.
- Establishing measures to ensure the integrity of the data and applications found within the owner's area of responsibility.
- Authorizing individual's appropriate security access rights for accessing the data and applications that are assigned to the data owner for administration.
- Periodically reviewing access rights to determine that the level is still appropriate for authorized users or the level needs to be changed.
- Assuring a process is in place to retain or purge information according to record retention schedules as set by the Records Management office of the Bureau of Administration or other entities.
- Determining the sensitivity and criticality of the data and application based on established Federal, State, and organizational definitions.

Compliance with system security and integrity; noncompliance and enforcement; reservation of authority and rights is expected of all employees and contractors.

- All State and contractor personnel utilizing information technology resources shall cooperate fully with the cyber security policies of the State.
- The State reserves the right to take all necessary actions to prevent the State network and computing infrastructure from being used to attack, damage, harm, or improperly exploit any internal or external systems or networks.
- The State reserves the right to take all necessary actions to protect the integrity of the State network, the systems attached to the State network, and the data contained therein.
- Violations of federal, State regulations, or any laws respecting information technology will be considered serious matters that may warrant loss of applicable privileges, fines, or more serious action as necessary, to include but not limited, appropriate disciplinary action.

Individuals with questions concerning the policies described herein should be directed to either an immediate State supervisor or the BIT Help Desk for assignment to the most pertinent BIT Division.

Compliance and Enforcement:

All managers and supervisors are responsible for enforcing the

Security Awareness policy. Any disclosure of regulated data is

subject to the Human Resource Polices of BHR.

1.1.2. Purpose

This Information Technology Security Policy contains information technology security policies to ensure that employees and contractors are familiar with the laws and regulations that govern use of IT systems and the data those systems contain.

1.1.3. Scope

The Information Technology Security Policy is intended to address the range of cyber security related topics. Detailed policies are listed and explained throughout the document. Security topics included are workstation, server, network, applications development, mobile, administrative, operational, and other IT areas.

The clientele served by BIT is very diverse. Including the Executive and Judicial branches of State government, local - municipal - county governments, K-12 schools, technical schools, and colleges and universities. Different policies will have a different set of impacted clienteles.

1.1.3.1. Scope Assumptions

The security policies listed within the Information Technology Security Policy apply to State employees and contractors working on or with State of South Dakota IT

equipment, data, or services. All are expected to comply with BIT cyber security policies.

1.1.3.2. Scope Constraints

Contractors are not given any special privileges or dispensations regarding policies listed herein. Contractors are expected to follow all policies designated as an employee would follow them. Third party hosting companies also have a set of policies applicable to them. This set of policies is normally a subset of the entire BIT catalog of policies.

1.1.4. Policy

1.1.4.1. General

The policy of BIT is that information is considered a valuable asset and must be appropriately evaluated and protected against all forms of unauthorized access, use, disclosure, modification, or destruction. Security controls must be sufficient to ensure the confidentiality, integrity, availability, and accountability of sensitive and critical information processed and stored on BIT resources and other hosting parties.

In addition to implementing the necessary safeguards, each State department, office, and agency is required to determine that the proper levels of protection for the information for that entity exists to include information that is under the control of the department, office, or agency. The security controls that must be applied will be consistent with the classification or value of the information and associated processes that the security controls are designed to protect. Information that is considered by management to be sensitive, critical, or sensitive and critical requires more stringent controls.

1.1.4.2. Chief Information Security Officer

The Commissioner of BIT shall appoint a Chief Information Security Officer (CISO) to implement the information technology security program for the State. The CISO shall seek to assure that information technology is secure at the State and shall be responsible for the following duties:

- Enforcing the provisions of the Information Technology Security Policy.
- Providing for and implementing, in cooperation with the Data Center, Development, and Telecommunications Divisions of BIT, a written process to investigate any violations or potential violations of this policy or any policy regarding system security and integrity, individually or in cooperation with any appropriate State law enforcement or investigative official.
- Implementing training and education programs to ensure government employees are aware of the risks and expected behaviors towards cyber security.
- Keeping a record of system integrity problems and incidents.
- Maintaining and updating the Information Technology Security Policies.
- Taking such emergency action as is reasonably necessary to provide system control where security is deemed to have been lost or jeopardized.
- Performing periodic security surveys.
- Providing for network security by seeking to preclude misuse of the network of the State to gain or attempt to gain unauthorized access to any system.
- Performing checks of information systems to assess system security and integrity, as well as to determine the use or placement of illegal or improper software or equipment.
- Coordinating the cyber security activities across BIT to ensure technology services and IT policies are effective in balancing security requirements vs. client needs.
- Ensuring processes are in place to remove all data before equipment is disposed or redeployed.
- Coordinating and consulting with the BIT Security Infrastructure Team (SIT), Executive Working Group on Cyber Security, other State departments, Board of Regents, K-12 community, federal Department of Homeland Security, and Multi-State Information Sharing and Analysis Center (MS-ISAC).
- Implementing decisions of the State concerning information technology security.
- Providing reports directly to the Office of the Governor where any serious security violation or potential challenge to security occurs.
- Leading the BIT Security Infrastructure Team.
- Leading the Executive Working Group on Cyber Security.

1.1.4.3. Security Infrastructure Team (SIT)

The SIT shall, in coordination with the CISO, recommend technology solutions, written policies, and procedures necessary for assuring the security and integrity of State information technology. The SIT shall coordinate with the CISO in creating and implementing a written system to investigate any violations or potential violations of this policy or any policy regarding system security and integrity.

- The CISO shall appoint the Security Infrastructure Team members.
- The SIT shall be chaired by the CISO.
- At a minimum, the SIT communicates internally every two weeks, via a scheduled bi-weekly meeting or via email, the current security posture of the State.
- The SIT shall consist of at least one member from each of the BIT information technology divisions.
- The recommendation is that membership include multiple representation from development, systems integration, desktop support, networking.
- K-12, Regental, Judicial, Legislative, and other government entities can be invited at the discretion of the CISO.

1.1.4.4. Security Operations Team (SOT)

The Security Operations Team (SOT) shall be appointed by the CISO. The SOT meets daily to review any cyber security findings or issues with the State Infrastructure within the previous day. The SOT includes members of the Telecommunications, Data Center, and Development divisions.

- Logs are fed into the State security information and event management system and are monitored by the SOT daily. These logs include firewall, intrusion detection, intrusion prevention, desktop protection, audit logs, etc.
- The SOT meets daily to review any findings or issues.
- Plans of action are established with assignments established based on the deficiencies.

The SOT can make recommendations and suggestions to the SIT for operational considerations.

1.1.4.5. BIT Executive Working Group on Cyber Security

The Executive Working group shall be informed and educated on matters regarding cyber security. They shall offer their perspective and feedback on technology, policies and other important matters.

- At the CISO's discretion, the members of the Working group shall come from the Executive, Judicial, Legislative branches of State government, constitutional offices, K-12 public schools and higher education, and other qualified individuals.

The Group shall meet quarterly at a minimum.

Administrative -I/T Asset Protection-Background Checks

10.1.1. Overview

As a condition of employment, all current and prospective Bureau of Information and Telecommunications (BIT) employees and Information Technology contractors desiring to work for the State shall be screened thoroughly including verification of qualifications.

Prospective employees and contractors will be notified that a background check will be done as part of the recruiting and selection process.

These verifications must be performed at least once every ten years.

10.1.2. Purpose

Ensure that current and prospective BIT employees and Information Technology contractors do not have a criminal history that would raise suspicion as to the integrity of their employment.

10.1.3. Scope

Background checks shall be limited to criminal history available through State and Federal resources.

10.1.3.1. Scope Assumptions

The scope includes BIT employees and prospective BIT employees of the Administration, Data Center, Development, and Telecommunications Divisions, South Dakota Public Broadcasting studio engineers, field engineers, and network operations center staff as well as current and prospective Information Technology contractors desiring to work for the State.

10.1.3.2. Scope Constraints

Background checks are not performed for financial or credit information.

10.1.4. Policy

10.1.4.1. Background Checks

BIT requires all current and prospective BIT employees, State Technology contractors, and the South Dakota Public Broadcasting Engineering group who write or modify State of South Dakota-owned software, alter hardware, configure software of State-owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas to undergo Federal fingerprint-based background checks and to have these background checks repeated at least once every ten years. Failure to comply with a federal background investigation may result in disciplinary action up to and including termination of employment or the rescinding of a conditional offer of employment.

These background checks must be fingerprint-based and performed by the State with support from the State's law enforcement resources. Under provisions set forth in Title 28, Code of Federal Regulations (CFR), Section 50.12, the prospective employees and contractors will be provided written notification that their fingerprints will be used to check the criminal history records of the State and the Federal Bureau of Investigation (FBI). Identification records obtained from the FBI may be used solely for the purpose requested and may not be disseminated outside the receiving department, related agency, or other authorized entity. BIT will supply the fingerprint cards and the procedure that is to be used to process the fingerprint cards.

Individuals should plan on the background check taking two to four weeks.

The steps to process the background checks are found in procedures document ITSP 1010.1 Background Checks Procedures.

10.1.4.2. Disqualifying Criteria

SDCL 1-33-63 allows the Commissioner of BIT to require a Federal background investigation be performed on any current or prospective BIT employee or Information Technology contractor that has access to confidential data or information. To implement these provisions, BIT must determine and memorialize its Disqualifying Criteria policy - the specific criminal activity that operates to disqualify a person from having access to the confidential data.

For purposes of this Policy, the terms "employee or contractor" means "potential or current BIT employee or Information Technology contractor."

A. An employee or contractor may not have access to confidential data if the individual has been convicted of a felony within 5 years of the date of the most recent criminal background check or any time thereafter.

1. Employees or contractors involved with technology associated with the division of the South Dakota Lottery must meet the qualifications defined in SDCL 42-7A-14. Primarily, this extends the period beyond completing felony sentencing to 10 years, rather than 5 as defined in A. above.

B. If the employee or contractor has been convicted of a crime not included in Paragraph A, the employee or contractor is not automatically disqualified from having access to confidential data. The determination of whether such an employee or contractor may have access to confidential data will be made on an individual basis. The considerations will include but not be limited to:
   1. The nature of the conviction, particularly if it is a crime of dishonesty, a financial crime, an identity crime, or a crime involving the misuse of confidential information.
   2. The length of time between the offense and the employment decision.
   3. The number of offenses.
   4. The relatedness of the conviction to the duties and responsibilities of the position.
   5. The efforts at maintaining a clean record.
   6. The number of crimes committed.

C. The determination required by Paragraph B will be made by the BIT Chief Information Security Officer (CISO) in consultation with the applicable Division Director.

D. Under no circumstances may an employee or contractor have access to confidential data if the individual is disqualified by this policy.

E. If a position within the BIT requires an employee or contractor to have access to confidential data as an essential part of the job function, the individual's failure to undergo or to successfully pass a criminal background check may result in termination of the employee or contractor.

F. After the adoption of this policy, no employee or contractor may be hired by BIT unless the individual undergoes and successfully passes a criminal background check pursuant to this policy.

G. The hiring of support staff positions and promotions within support staff positions may be excluded from this policy.

10.1.4.3. Noncriminal Agency Coordinator (NAC)

The CISO is designated as a Noncriminal Agency Coordinator (NAC) to act as the primary contact person for BIT.

10.1.4.4. Local Agency Security Officer (LASO)

The CISO is appointed as a Local Agency Security Officer (LASO) to act as liaison with the South Dakota Division of Criminal Investigation (SDDCI) to ensure the BIT follows security procedures.

10.1.4.5. Background Check Interpretation

When an explanation of a charge or disposition is needed, the BIT NAC will communicate directly with the agency (SDDCI) that furnished the data to the FBI.

10.1.4.6. Not Guilty Presumption

An individual should be presumed not guilty of any charge/arrest for which there is no final disposition stated on the record or otherwise determined.

10.1.4.7. Background Check Information Challenge

An opportunity to challenge and discuss the disqualification due to information found in the criminal history records of the FBI will be provided to the applicant for five days, if requested. Due to the confidential nature of the criminal history records of the FBI and the restrictions on disclosure of the records, it may be discussed that the applicant was disqualified because of criminal history information; however, the specific FBI results may not be disclosed to the applicant, neither in writing nor verbally.

Under provisions set forth in Title 28, CFR, Section 50.12, if the information on the record is used to disqualify an applicant, the official making the determination of suitability for licensing or employment shall provide the applicant the opportunity to complete, or challenge the accuracy of, the information contained in the FBI Identification record. The deciding official should not deny the license or employment based on the information in

the record until the applicant has been afforded a reasonable time to correct or complete the information or has declined to do so.

10.1.4.8. Corrective Action

If the applicant wishes to correct the record as it appears in the FBI's Criminal Justice Information Services (CJIS) Division Records System, the applicant should be advised that the procedures to change, correct, or update the record are set forth in Title 28, CFR, Section 16.34.

10.1.4.9. Training

BIT will comply with mandatory training requirements as outlined in the South Dakota Division of Criminal Investigation Guide for Noncriminal Justice Agencies. All personnel directly associated with accessing, maintaining, processing, dissemination, or destruction of Criminal History Record Information (CHRI) shall be trained.

10.1.4.10. Emailing Background Check Information

It is prohibited to mail criminal history background check information either as an email or as an attachment to email. Individuals are prohibited from opening any email that contains background check information. They must report the occurrence to their supervisor and delete the email.

Administrative -I/T Asset Protection-Confidentiality

10.3.1. Overview

All BIT employees and contracted technology professionals shall be granted appropriate access to information, agency documents, records, programs, files, diagrams, and pertinent data resources needed to fulfill the job responsibilities of an individual or a contractual agreement. In return, it is expected that such data is treated as a trade secret and individuals will not modify data or disclose data to others without proper authorization. Products resulting from employment or custom-built solutions for government agencies are the property of the State.

10.3.2. Purpose

To ensure that employees are familiar with the laws that govern use of information technology systems and the data contained within those systems and that employees and contractor comply with such laws.

10.3.3. Scope

This policy applies to BIT and technology contractors of the State. It includes the protection of sensitive data in addition to the work products built under State guidance.

Individuals shall maintain confidentiality and data integrity of documents, records, configurations, programs, and files and understand that work products resulting from such efforts are the property of the State.

10.3.3.1. Scope Assumptions

The confidentiality and data integrity responsibility of BIT employees and contractors extends to, but is not limited to systems, software, data, configurations, architectures / designs, documentation, and infrastructure information developed on its own or acquired from third parties. Customized work products including specific-built software solutions are the property of the State.

10.3.3.2. Scope Constraints

Agencies will have their own data protection and confidentiality agreements. Leased and licensed software is exempt from this policy.

10.3.4. Policy

10.3.4.1. Confidentiality Agreement

The individual must not, at any time, use or disclose any trade secrets or confidential information of the State to anyone, include agencies or contractors that have business with the State, without written permission from the BIT Commissioner, except as required to perform duties for the State.

The individual agrees to adhere to all data processing and technology policies governing the use of the technology infrastructure of the State.

The individual agrees that all developments made and works created by the individual in connection with the contractual agreement of the State shall be the sole and complete property of the State, and all copyrights and other proprietary interest, therein, shall belong to the State.

Upon the request of the State to include the termination of the employment of the person, the individual will leave all reports, messages, programs, diagrams, documentation, code, memoranda, notes, records, drawings, manuals, flow charts, and any other documents whether manual or electronic pertaining to the State, including all copies thereof, with BIT to include all data resources whether manual or electronic involving any trade secrets or confidential information of the State to include agencies or contractors that have business with the State.

Complying with Legal Obligations

Employees and contractors are subject to Federal, State and local laws governing the use of information technology systems and the data contained in those systems.

- BIT shall comply with all applicable laws and take measures to protect the information technology systems and the data contained within information systems. Agencies must take the initiative to comply with applicable laws and regulations pertaining to their field of business.
- BIT shall ensure that all BIT employees and technology contractors are aware of legal and regulatory requirements that address the use of information technology systems and the data that reside on those systems.
- Agencies shall ensure that each public employee and other agency authorized users are provided with a summary of the legal obligations that apply to that agency such as HIPAA, etc.

10.3.4.2. Security Acknowledgement and Access

Once chosen, contractors must identify all individual contractors that will be participating in work for the State and begin participating after the work has begun.

Contractors working with the State shall be required to sign the *Security Acknowledgement form* (http://intranet.bit.sd.gov/forms/).

All BIT employees and contractors need to have a copy signed and filed. Contractor access to the technology infrastructure of the State is closely managed and limited.

Contractors do not have the same degree of access nor privileges given to State employees.

At the sole discretion of BIT, access for a contractor to the technology infrastructure of the State can be amended or terminated.

Mainframe-Mainframe Security-Mainframe Accounts

210.3.1. Overview

This policy covers the mandatory use of individual User IDs to control access to specific mainframe resources.

210.3.2. Purpose

To protect mainframe resources from unauthorized or inappropriate access unique User IDs are used. Rights are granted case-by-case allowing for auditing of both successful and unsuccessful access attempts that can be tracked for security audits.

210.3.3. Scope

Mainframe security requirements apply all those who have access to or use mainframe resources administered by BIT.

210.3.3.1. Scope Assumptions

This policy applies to those who use or wish to use and/or have access to mainframe resources.

210.3.3.2. Scope Constraints

This policy applies to only to those who wish or do use or access any mainframe resources. It does not necessarily apply to resources on Windows, Unix, or AS/400 platforms.

210.3.4. Policy

210.3.4.1. Unique Account Requirement

All mainframe resources are protected by one or more mainframe security systems. Each individual that requires access to mainframe resources must have a unique User ID which allows for viewing, updating, creating or deleting of protected resources controlled by least one of the security systems.

210.3.4.2. Requests for Mainframe User IDs

Access to mainframe systems and data is granted only when a specific business need is proven, as defined by BIT client departments and BIT Mainframe Security Administration. All access for department personnel must be requested in writing to the BIT Help Desk using the *Employee Request Form (New/Move)* at the BIT Intranet http://intranet.bit.sd.gov/forms. All requests must be made by department personnel authorized to make such requests and access will be assigned based on the principle of least privilege, which requires that a user be given no more privilege than necessary to perform a job.

210.3.4.3. Responsibility for Mainframe UserIDs and Passwords

All client user access to mainframe resources is identified by assigned mainframe User IDs and authenticated by passwords. Individuals that have been assigned an individual mainframe User ID are considered the owner of the ID and are responsible for securing and protecting its password. Individuals must not write the password on paper, post the password on terminals, save the password in computer files or allow the password to be known by other individuals. Individuals on record as being the owner of an ID are responsible for all valid or invalid access made by that ID. Unauthorized access to State or Federally protected data may be prosecuted by State and Federal authorities.

Mainframe-Mainframe Security-Mainframe Accounts

210.4.1. Overview

This policy covers the mandatory use of individual User IDs to control access to specific mainframe resources.

210.4.2. Purpose

To protect mainframe resources from unauthorized or inappropriate access unique User IDs are used. Rights are granted case-by-case allowing for auditing of both successful and unsuccessful access attempts that can be tracked for security audits.

210.4.3. Scope

Mainframe security requirements apply to all those who have access to mainframe resources administered by BIT.

210.4.3.1. Scope Assumptions

This policy applies to those who use or wish to use and/or have access to mainframe resources.

210.4.3.2. Scope Constraints

This policy applies to only to those who wish to or do use or access any mainframe resources. It does not apply to resources on Windows, UNIX or mobile devices.

210.4.4. Policy

210.4.4.1. Mainframe User ID Revocation

Mainframe user IDs will be disabled if they are not used within forty-five days and will need to be reset by the BIT Help Desk.

Mainframe-Mainframe Security-Mainframe Access

210.25.1. Overview

This policy covers requirements that must be met before physical access will be granted to the BIT Computer Room.

210.25.2. Purpose

The purpose of this policy is to protect physical mainframe resources from unauthorized access through the use of physical access requirements.

210.25.3. Scope

These security requirements apply those who have a need to gain physical access to the location that houses mainframe hardware administered by the BIT.

210.25.3.1. Scope Assumptions

The policy applies to those who wish to gain physical access to the BIT Computer Room.

210.25.3.2. Scope Constraints

This policy applies to only to those who wish to access the BIT Computer Room. It does not necessarily apply to other facilities or rooms administered by BIT personnel.

210.25.4. Policy

210.25.4.1. Mainframe Access

For security reasons, BIT maintains what is referred to as a "closed" computer room. No individuals, other than BIT Operations personnel, are permitted in the mainframe computer room unless the person can show a need to be in the room, provide a form of photo identification, and sign in and sign out. Individuals who meet these requirements must also be escorted by Data Center staff at all times.

Server-Server Security-Server Maintenance and Administration

220.1.1. Overview

Servers require maintenance. Failure to maintain a server exposes the State to unacceptable security risks. Allowing server patching status to be visible outside a network can also expose the network to unacceptable risk. Out-of-date systems that are accessible from the Internet may have vulnerabilities related to the application servers or the application framework. There can be design flaws or implementation bugs. Hackers look for evidence of weak links in cyber defenses. A successful exploitation may result in data loss, bad reputation, loss of credibility, or financial problems.

220.1.2. Purpose

This empowers BIT to manage State enterprise servers and provide for secure server maintenance on any network State data and applications reside.

220.1.3. Scope

This policy covers BIT managed enterprise servers, Contractor managed servers connecting to the State network, and Contractor managed networks that host State data and/or applications.

220.1.3.1. Scope Assumptions

A server is connected to the State network or hosts state data and/or applications.

220.1.3.2. Scope Constraints

This only applies to the State's enterprise distributed system that hosts state data and/or applications. This policy does not include the State mainframe, AS/400, desktop, and mobile devices.

220.1.4. Policy

220.1.4.1. Visibility of Server and Framework Patching Status

The server patch status will not be visible outside a network hosting State data and/or application. This policy applies to both the State network and Contractor networks that host State data or applications.

Server-Server Security-File Transfer Protocol

220.7.1. Overview

The State supported FTP server is meant for short term storage only and is not meant as a permanent data store. The FTP service should be used for applications uploading or downloading files that have a limited lifespan, transfer of files of large size, and temporary placement for files to be downloaded outside the technology infrastructure of the State. The FTP server is not backed up and all files placed on the server have a lifespan of seven days. If the files are not removed after seven days, the data will be automatically deleted. The FTP server is secured to the Internet; in order for outside entities to get into the FTP server, an FTP username and password is required. In addition, the FTP server is secured from internal clients of the State though the configuration of the permissions for the device. By default, all State users have Read, Write and Delete access while internet users have no access.

- All access will require a user id and password. Anonymous FTP is not acceptable.
- Retention period on all files will be limited to seven calendar days. Individual files will be deleted after seven days of storage.

220.7.2. Purpose

To limit the volume of data storage on the FTP server and assure the FTP server serves the purpose for which it is intended, namely a reliable way to temporarily store data that is being transferred into our out of the state.

220.7.3. Scope

The scope is the use of the State's FTP server within the State domain.

220.7.3.1. Scope Assumptions

This policy only covers only the State's FTP server within the State domain.

220.7.3.2. Scope Constraints

This policy only applies to the State's FTP server and its use as a temporary storage location. It does not apply to any other data storage locations or data-transfer processes.

220.7.4. Policy

220.7.4.1. Use of File Transfer Protocol Server

Internet users shall use the available FTP software to get to the FTP server. The FTP server is meant for short term storage only and is not meant as a permanent data store. Copying or retrieving files from the FTP server by Internet clients is not allowed unless an account is created for the individual or company. Contact the BIT Help Desk to

request access to the available FTP software and/or the steps, costs, and authorizations required to create an FTP account for a non-State user.

Server-Server Security-Assurance HIPAA Regulations are Met

220.10.1. Overview

BIT will establish and maintain the security and privacy of electronic Health Insurance Portability and Accountability Act (HIPAA) information created, used, transmitted, stored, and destroyed by State employees and/or the State in accordance with Federal laws and regulations.

220.10.2. Purpose

Ensure HIPAA regulations covered by title 45 of the Code of Federal Regulations (CFR) Part 160 and Part 164 are met.

220.10.3. Scope

This policy applies to those who access or create HIPAA data on systems managed by BIT.

220.10.3.1. Scope Assumptions

You use HIPAA data in electronic form, electronic Personal Information (ePHI).

220.10.3.2. Scope Constraints

This policy only applies to users of HIPAA data in electronic form (ePHI).

220.10.4. Policy

220.10.4.1. The Data User is Responsible for Adhering to HIPAA Regulations

Each user with access to HIPAA data is responsible for understanding federal requirements for data handling and security and accountable for any actions they take that may compromise the security or confidentiality of HIPAA data. BIT will work with HIPAA authorized agency staff and authorized federal audit staff as well as written federal rules and regulations to assure security and access controls are in place to meet 45 CFR Part 160 and Part 164 and other applicable rules and regulations relating to electronic HIPAA information created, used, transmitted, stored, and destroyed on technology managed by BIT. Where deficiencies are determined to exist, BIT will work with the appropriate resources within the State and the applicable federal audit group to address those.

Data Center General-Data Center Security-Cloud Based Services and System Information

230.9.1. Overview

Cloud-based technology providers rely on a wide range of technologies and business models to offer and maintain their services. The security, reliability, portability, resilience, and long-term viability of any given service offering is largely dependent on the technologies and business models in use and the manner in which those technologies and business models are implemented, maintained, and managed.

However, it is impossible to know what the nature of the underlying technologies or business practices may be without a collaborative, detailed, and thoughtful review with the cloud-based technology provider.

BIT must approve and be a signatory to all cloud-based and remote technology service and system agreements.

230.9.2. Purpose

Define BIT's authority to review, approve, and be a signatory to cloud based systems and technology services agreements used or contracted for by client agencies.

230.9.3. Scope

The scope of this policy includes all executive branch technology acquisitions that use any cloud-based system or service that originates from outside the direct physical or logical control and management of BIT.

230.9.3.1. Scope Assumptions

This policy applies to any cloud-based system or services used or acquired by an agency that originates from outside the direct physical or logical control and management of BIT.

230.9.3.2. Scope Constraints

This policy does not apply to third party systems or services that are hosted at the state on BIT managed infrastructure and/or managed by BIT. This policy does not apply to systems or services for the State's K-12 or clients.

230.9.4. Policy

230.9.4.1. Responsibility for Cloud Based Services and Systems.

As the approving entity for all statewide IT services and systems, including cloud-based services and systems, BIT must review, approve, and be a signatory to all agreements for acquiring or using cloud-based types of systems or services. Cloud-based technology providers include, but are not limited to, any entity that uses technologies and business processes to store, access, or manipulate state or citizen data from outside the direct physical or logical control and management of BIT managed systems.

It is critical to plan ahead for the purchasing of these services from an IT or cloud provider. Agencies must factor in the time required for BIT staff to perform a detailed review and assessment to determine whether approval can be granted.

Data Center General-Secure Information Technology Acquisition Policy- Secure Information Technology Acquisition Policy

230.10.1. Overview

Secure information technology acquisition is the methodology the State uses to acquire information technology goods and services. The goal is to acquire I/T goods and services that meet security and technology standards as inexpensively as possible. To that end there must be processes that filter out insecure technology that does not meet State standards, identify solutions that are technological unsound and discover all cost associated with the acquisition. These processes must work in conjunction to

accomplish those ends. This must be accomplished while recognizing the sometimes-unique needs of BIT's clients and encouraging their full participation in the process.

230.10.2. Purpose

The purpose is to acquire I/T goods and services as securely as possible.

230.10.3. Scope

These policies cover the acquisition of I/T goods and services by the executive branch and any other branch or entity acquiring technology that will be used on or with the State's I/T infrastructure.

230.10.3.1. Scope Assumptions

These polices assume that you are acquiring I/T related goods and/or services.

230.10.3.2. Scope Constraints

These policies only apply to the acquisition of I/T goods and services.

230.10.4. Policy

230.10.4.1. Hardware Maintenance Agreements

Any hardware acquired must include a commitment by the supplier to keep the hardware's associated software and firmware patched and up-to-date as well as providing a hardware maintenance agreement. BIT will scan all hardware and the software and firmware associated with the hardware for security vulnerabilities on a regular basis and will apply vendor-supplied mitigation for any vulnerabilities found. When a hardware reaches the vendor's end-of-life date, BIT will continue scanning the hardware and will mitigate any new vulnerabilities found, up to and including replacing the hardware if the vulnerability is severe enough and if there is no other mitigation available.

Data Center General-Data Center Security-Federal Tax Information

230.11.1. Overview

This policy covers safeguarding Federal Tax Information (FTI). Special handling instructions must be in place when working with FTI including the prohibition of remote access to FTI without using multi-factor authentication. This policy documents what is FTI, what is not, and what safeguards must be implemented specific to files that contain FTI.

230.11.2. Purpose

To define FTI as well as the safeguards that must be in place when receiving, handling, or sharing FTI.

230.11.3. Scope

This policy applies to all FTI obtained directly from the Internal Revenue Service (IRS) or from an official IRS form.

230.11.3.1. Scope Assumptions

It is assumed that individuals receiving and/or accessing FTI have a legitimate business need to do so, and have obtained the necessary permissions from the IRS to transfer information of this nature to State-owned servers and/or to access information of this nature.

230.11.3.2. Scope Constraints

This policy applies only to Federal Tax Information. This policy does not apply to information that is not FTI.

230.11.4. Policy

230.11.4.1. Federal Tax Information Returns and Return Information

A return is any tax or information return, estimated tax declaration or refund claim to include amendments, supplements, supporting schedules, attachments or lists required by, and filed with the IRS by, on behalf of, or with respect to any person or entity. Examples of returns include forms filed on paper or electronically, such as Forms 1040, 941, 1120, and other informational forms, such as 1099 or W-2. Forms include supporting schedules, attachments or lists that are supplemental to or part of such a return.

Information collected or generated by the IRS regarding a person's Internal Revenue Code liability or potential liability includes but is not limited to:

- Information, including the return, that IRS obtained from any source or developed through any means that relates to the potential liability of any person under the IRC for any tax, penalty, interest, fine, forfeiture, or other imposition or offense.
- Information extracted from a return, including names of dependents or the location of business, the taxpayer's name, address, and identification number.
- Information collected by the IRS about any person's tax affairs, even if identifiers such as name, address, and identification number are deleted.
- FTI may include PII. FTI may include the following PII elements, the:
    - Name of a person with respect to whom a return is filed.
    - Mailing address.
    - Taxpayer identification number.
    - Email addresses.
    - Telephone numbers.
    - Social Security Numbers.
    - Bank account numbers.
    - Date and place of birth.
    - Mother's maiden name;
    - Biometric data (e.g., height, weight, eye color, fingerprints).
    - Any combination of the preceding.

If the preceding information needs clarification or should ever come in question, BIT will review and define FTI as Federal Tax Information as defined within the tax codes of the United States of America by accessing www.irs.gov to search for Tax Code, Regulations and Official Guidance. For the purpose of BIT security planning anything stored on mainframe media is treated as if the media contains FTI.

230.11.4.2. What is Not Federal Tax Information

FTI does not include information provided directly by the taxpayer or third parties. If the taxpayer or third party subsequently provides returns, return information or other PII independently, the information is not FTI as long as the IRS source information is replaced with the newly provided information.

230.11.4.3. Safeguarding Federal Tax Information

Safeguarding FTI is critically important so confidential taxpayer information is continuously protected as required by federal law. Access to FTI is permitted only to

individuals who require the FTI to perform their official duties and as authorized under the IRC. FTI must never be indiscriminately disseminated, even within State government.

230.11.4.4. Emailing Federal Tax Information

It is prohibited to email FTI either as an email or as an attachment to an email. Do not open any email that contains FTI but report the occurrence to your supervisor and delete the email.

Data Center General-Procedural-Physical Access - Proximity Cards

230.58.1. Overview

This policy addresses the issuance, use, and monitoring of proximity cards which provide access to BIT facilities.

230.58.2. Purpose

Physical access to equipment facilities controlled by BIT must be restricted to authorized personnel only.

230.58.3. Scope

Authorized personnel may be BIT employees, BIT contractor personnel, or other State personnel that have equipment located in BIT facilities.

230.58.3.1. Scope Assumptions

Staff and visitors have a legitimate business need for entering BIT facilities.

230.58.3.2. Scope Constraints

This policy does not apply to locations equipped with proximity card readers that are not maintained by BIT.

230.58.4. Policy

230.58.4.1. Proximity Card for Non-BIT Employee Access

Temporary Guest Access

On occasion, situations may exist where a contractor needs to have temporary access to a secured environment. Authorized visitors must provide their escort with a photo ID and the guest and escort must jointly sign in using the sign in sheets located inside the door of each equipment facility. The individuals are guests of the State and must be monitored at all times by an authorized employee of BIT. The individuals cannot be left alone in a secured location without supervision. Only BIT employees with access privileges to the secured facility being accessed are authorized to be an escort for visitors.

Permanent Access Procedures for Non-BIT Employees

Contractors and other agency personnel that have been issued a proximity card are considered trusted partners. However, trusted partners do not have the authority to sign in visitors that have not been issued a proximity card.

Access to the state campus tunnel system
All agencies follow the process and policies regarding tunnel system access on the state campus as set and managed by the Department of Public Safety (DPS). BIT shall support the policy and follow its requirements and processes as defined and as directed by DPS.

Data Center General-Data Center Security-Accounts Access Control and Authorization

230.67.1. Overview

All devices that can connect to the State domain and/or managed by BIT as well as their peripheral devices will have security policies established and implemented to restrict unauthorized activities. Authorization for individuals to access programs, databases, and related technologies will be enforced. Access must be based on least privilege. Individual accounts are created for those with a need to access State IT resources. Access must end

when the manager of an employee or contractor determines access is no longer required or when job responsibilities change, and privileged access must be adjusted. Only authorized personnel will be allowed to change passwords and they must have proper credentials to prove who they are.

There are policies for thresholds for lockouts, duration of lockouts, and resets specific to the Department of Human Services (DHS), Department of Revenue (DOR), Department of Social Services (DSS), and the Department of Labor and Regulation (DLR).

230.67.2. Purpose

This policy provides the forms and processes to authorize, create, maintain and terminate accounts.

230.67.3. Scope

This policy covers all State IT resources managed by BIT.

230.67.3.1. Scope Assumptions

Employee and contractor access are authorized by an immediate supervisor or higher-level manager. Security administrators will conduct periodic reviews to verify that only access needed by an individual's job duties have been assigned. When a supervisor or manager determines access needs to be changed, they must notify BIT using the Employee Request Form (New/Move/Change Responsibilities).

230.67.3.2. Scope Constraints

This policy does not apply to the mainframe, the AS/400s, or IT resources which are not managed by BIT. The lockout threshold, lockout duration, and reset requirements apply only to DHS, DOR, DSS, or DLR workstations.

230.67.4. Policy

230.67.4.1. Individual Access Authorization

The Employee Request Form (New/Move/Change Responsibilities) is used to request access to State IT resources and it must be filled out by an authorized manager. This form must be used when a contractor starts, a new employee is hired, an employee transfers positions, or when an employee's or a contractor's duties change. If the change in duties is enough to regard the change as a new position or requires a new or amended contract the Security Acknowledgement form must also be signed.

230.67.4.2. Least Privilege

Access privileges must be layered to reflect job functions and separation of duties, and minimal security privileges or only the security privileges required for an individual to perform work duties must be assigned.

230.67.4.3. Password Requirements

Must:

- Be changed every ninety days.
- Be at least eight characters.
- Contain at least three of the following four-character groups:
    - English uppercase characters (A through Z).
    - English lowercase characters (a through z).
    - Numerals (0 through 9).

- Non-alphabetic characters (such as !, $, #, %).

- Must not be one of the twenty-four most recent passwords;
- Must not have been changed within the last seven days.
- Does not contain first name. last name, username.
- Does not contain Social Security Number.
- Does not contain permutations of "password".
- Cannot be a dictionary word.

User accounts with no administrative rights will need to change their passwords every 90-days. User accounts with administrative rights will need to change their passwords every 60-days. Where existing State technology products can support multiple expiration password policies for individual administrators' accounts that have administrative access rights without altering the general 90-day expiration password policy for individual users' accounts that do not have administrative access rights, the expiration password policy shall be set to 60-days for such administrators' accounts that have administrative access rights. Contractor passwords that provide access to the State's system or devices must expire after 60-days. Contractor(s) must not share passwords with other contractor(s).

230.67.4.4. Individual Access Termination

Access privileges must be terminated immediately when authorization ends for a user identified by the individual's manager. When an employee or contractor employment is terminated, the manager is responsible for completing the Exiting Employee Request form. If the termination is immediate, the BIT Help Desk (605-773-4357) must be notified without delay so that access and authorization assigned to the individual can be disabled. In all departing employee situations, managers must take reasonable steps to ensure no assets of the State including data, software, or hardware are taken, shared, inappropriately modified, or destroyed by the individual.

Data Center General-Payment Card Industry Data Security-Payment Card Industry Data Security Standard

230.72.1. Overview

Payment Card Industry Data Security Standard (PCI) requirements are set by the Payment Card Industry Security Standards Council to protect cardholder data. The standards govern all merchants and organizations that store, process, or transmit this data, and include requirements for software developers and manufacturers of applications and devices used in the transaction process. Compliance with the PCI security standards is enforced by the major payment card brands who formed the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI compliance is required of all merchants and service providers that store, process, or transmit cardholder data. The requirements apply to all payment methods, including retail (in person), mail/telephone order, and e- commerce. Failure to adhere to PCI

standards can result in the State not being able to use payment cards and can result in fines.

230.72.2. Purpose

The purpose is to ensure the State complies with PCI security standards.

230.72.3. Scope

These policies cover the servicing of payment cards for goods and/or services provided by the State.

230.72.3.1. Scope Assumptions

Payment cards are used to reimbursement the State for goods and/or services provided by the State.

230.72.3.2. Scope Constraints

This policy covers payments made to the State not use of the State of payment cards to acquire goods and services.

230.72.4. Policy

230.72.4.1. Payment Card Industry Data Security Standard Requirements

The State is required by the payment card association to follow the PCI security standards. These standards assure a secure environment for our customers, protecting them against both loss and fraud. The State must comply with PCI requirements for securely processing, storing, transmitting, and disposing of cardholder data. Annually all payment card service providers (such as banks) that perform card processing for the State must be certified as PCI compliant. The service providers must submit a letter to BIT confirming compliance with PCI standards.

Data Center General-Secure Information Technology Acquisition Policy- Secure Information Technology Acquisition Policy

230.73.1. Overview

Secure information technology acquisition is the methodology the State uses to acquire information technology goods and services. The goal is to acquire I/T goods and services that meet security and technology standards as inexpensively as possible. To that end there must be processes that filter out insecure technology that does not meet State standards, identify solutions that are technologically unsound and discover all cost associated with the acquisition. These processes must work in conjunction to accomplish those ends. This must be accomplished by recognizing the unique needs of BIT's clients and encouraging their full participation in the process. BIT acquisition resources can be found on the BIT Technology Review webpage.

230.73.2. Purpose

The purpose is to acquire I/T goods and services as securely as possible.

230.73.3. Scope

These policies cover the acquisition of I/T goods and services by the executive branch and any other branch or entity acquiring technology that will be used on or with the State's I/T infrastructure.

230.73.3.1. Scope Assumptions

These polices assume that you are acquiring I/T related goods and/or services.

230.73.3.2. Scope Constraints

These policies only apply to the acquisition of I/T goods and services.

230.73.4. Policy

230.73.4.1. Acquisition of Services Involving HIPAA Data

Any contractor providing services that potentially can expose HIPAA data to the contractor, must sign the BIT business associate agreement before the work can start. If having the contractor sign a BIT business associate agreement is not possible or if it is thought that a business associate agreement is not needed, permission to proceed with the work must be obtained from the BIT Chief Information Security Officer before any work can proceed. There also must be a risk assessment performed by the BIT Chief Information Security Officer or a designee. There are no exceptions to these policies.

230.73.4.2. Security Scanning Requirements

Applications installed on the State's system or service(s) hosted by a contractor such as SaaS, PaaS or IaaS, must be scanned for security vulnerabilities. For any application, installed on either the State's infrastructure or the Contractor's, where a contract has not been signed, an authorization to scan must be signed before scanning can be done. Any exceptions to this policy must be approved by the BIT Chief Information Security Officer and may require a signed release by the agency recognizing the risks involved.

230.73.4.3. Hardware Maintenance Agreements

Any hardware acquired must include a commitment by the supplier to keep the hardware's associated software and firmware patched and up-to-date as well as providing a hardware maintenance agreement. BIT will scan all hardware and the software and firmware associated with the hardware for security vulnerabilities on a regular basis and will apply vendor-supplied mitigation for any vulnerabilities found. When a hardware reaches the vendor's end-of-life date, BIT will continue scanning the hardware and will mitigate any new vulnerabilities found, up to and including replacing the hardware if the vulnerability is severe enough and if there is no other mitigation available.

Data Center General-Use of Production Data-Use of Production Data in a Non-Production Environment

230.74.1. Overview

Precautions must be taken when copying data from a production environment to a non-production environment. A non-production environment can be, but is not limited to, staging, development, or test environments. State employees must store State data in non-production environments securely and must have approval before they move any protected production data to a non-production environment.

230.74.2. Purpose

This policy states how protected production data should be handled outside of production environments. The testing of applications can be enhanced with the use

of live data. Precautions must be taken insure that the protected data is safeguarded.

230.74.3. Scope

This policy includes all non-production environments that store, or process protected production data on State systems and the movement of State data to and from a contractor infrastructure. Movement of data on infrastructure completely outside the State's control by a Contractor is not covered by this policy. Movement of data on infrastructure outside the State's control by a Contractor will be governed by any agreements made between the State and the Contractor

Approval is obtained by using the BIT Moving Live Data Request Form. Any data protected under Federal
or State regulation or statute or industry standard is considered protected data. Protected data includes but is not

limited to Personally Identifiable Information (PII), Protected Heath Information (PHI), Federal Tax Information FTI), Family Educational Rights and Privacy Act (FERPA), Criminal Justice Information System data (CJIS), The Federal Parent Locator Service (FPLS), and Payment Card Industry data (PCI). Protected production data that is masked, deidentified or aggregated is no longer considered to be protected data. Information on what is legally protected data that is Personally Identifiable Information (PII) is found here.

230.74.3.1. Scope Assumptions

This policy assumes State employees and contractors are authorized to work with the data and need to move protected production data into:

- A non-production State environment.
- A Contractor environment.
- From a Contractor environment to a State environment.

230.74.3.2. Scope Constraints

This policy only covers State production data that will be moved into a non-production environment.

230.74.4. Policy

230.74.4.1. Use of Production Data in a Non-Production Environment

Approval must be obtained before moving protected production data to a non-production environment. The non- production environment must have the same level of security as the production environment. The BIT Moving Live Data Request Form must be used for approval. Contractors can obtain the form from their agency contact.

Approval for moving protected production data is valid for six months. If the data is needed in the non-production environment longer than the approval period, another BIT Moving Live Data Request Form must be filled out and approved before the last approval expires. An expedited approval can also be requested through the Moving Live Data Request Form for data that will only be in the non-production environment for two-business days or less. All data must be purged before either approval expires.

Prior to moving production data from the State's environment to the Contractor's system there must be a security scan. This scan must be done by the State or a BIT approved third-party. This scan can be done up to three- months before the data is moved. If there is a third-party scan the scan results must be provided to the State contact. An acceptable security scan report of the data must consist of a least:

- The system that was evaluated (URL if possible, mask if needed);
- The categories that were evaluated (for example SQL injection, cross site scripting, etc.);
- What were the general findings (for example how many SQL injection issues were found and the count per category);
- Technical details of each issue found including, where it was found, web address, what was found, and the http

response if possible.

The infrastructure scan report must include at least:

- What software, platform and framework were used to perform the scan;
- What general categories were evaluated, host discovery, vulnerability scan, external vulnerability scan or compliance checks;
- Explain the exact details of the test run with those categories;
- General findings or summary report;
- Technical findings, including the exact details of what was found and their severity.

The use of Federal Tax Information (FTI) in non-production environments requires authorization from the IRS Office of Safeguards by filling out the IRS Live Data Testing Notification Form. A copy, or link, to the approved IRS form must be attached to the BIT Moving Live Data Request Form. The use of FTI production data in a non-production environment is limited to tax administration or other authorized IRS purposes including:

- Testing new systems.
- Validation of Federal data load.
- Data matching between state and federal forms.
- Testing audit selection.

FTI data may only be disclosed to those requiring the data to perform their official duties. The requester may also be required to sign a form, provided by the data owner, prior to obtaining access to the production FTI. IRS approved sanitization methods must be used after the data is no longer needed.

The FPLS can be a secondary source of FTI. FTI from the FPLS is treated as if the FTI was from the IRS. Other forms of data that have unique requirements are:

- CJIS data can only be moved by the Office of Attorney General (ATG), it cannot be moved by BIT. The ATG must notify the CISO when CJIS data is moved, provide the location of that data, and inform the CISO if dual authorization is required before disposal of the data. After the CJIS data is no longer needed it must be disposed of as stated in ITSP 230.68. The documentation and verification of the disposal of the data will be completed by the ATG.
- PCI data may not be used in non-production environments.

Contractors with access to protected data must sign the Security Acknowledgement Form and have passed a background check before they can have access to the data.

Protected State data cannot be moved outside the United States of America or its territories.

The Data Center may be requested to verify compliance using, but not limited to, business tool reports, internal, and external audits. The request to verify can be made by the data owner or CISO.

230.74.4.2. Purging of Data

If there is unapproved protected production data in a non-production environment, the data must be purged. Any protected production data on a BIT-developed system that was moved to a non-production environment prior to this policy going into effect must be approved or purged. Any protected production data on BIT-hosted Contractor-developed system that was moved to a non-production environment prior to this policy going into effect must be approved by November 7, 2018 or purged.

Protected production data must be purged from the non-production environment before the BIT Moving Live Data Request Form approval has expired or it must be re-approved. It is the responsibility of the requestor of the data move to verify that the data has been purged.

230.74.4.3. Compliance

If an individual finds unapproved, unmasked protected production data in a non-production environment, they must:

1. Notify her or his manager.
2. The manager must notify the Development Director and CISO.
3. The data must be purged.
4. The Development Director and CISO will be notified when it is purged.

If unapproved, unmasked, protected production data is found in a non-production environment, the CISO will decide if it is a security incident. The individual(s) responsible for unapproved unmasked protected production data in a non-production environment may be subject to disciplinary action up to and including dismissal. The placing of unapproved unmasked FTI, HIPAA, or FPLS data on a non-production environment may subject the responsible individual to legal action as stated in IRS 1075 or The American Recovery and Reinvestment Act of 2009.

Data Center General -Security Impacts-Data Classification

230.75.1. Overview

Data classification establishes the agency and BIT responsibilities for handling, maintaining, and meeting required levels of security control for the data.

230.75.2. Purpose

The purpose of this policy is to provide data classification for confidentiality, integrity, and availability.

230.75.3. Scope

These policies include all State data located on State infrastructure or Contractor infrastructure. These policies also include data owned by Contractors if the data is used by an agency and resides on BIT managed systems. An example is Geographic Information System data. While the data may be owned by the Contractor the agency is considered the data owner for the purposes of these policies. If the data is owned by the Contractor and there are data handling requirements in the contract, the contractual data handling requirements preempts these policies.

230.75.3.1. Scope Assumptions

These policies cover all state data residing on the State's or a Contractor's system and Contractor data residing on State systems. Contractor owned data on a Contractor's system is not included.

230.75.3.2. Scope Constraints

These policies are limited to data and does not cover applications.

230.75.4. Policy

230.75.4.1. Data Classification System

Each agency shall serve as a classification authority for the data and information for which it is considered the data owner. BIT is not the data owner of data it collects or maintains for another State agency to fulfill that agency's mission; the State agency is the data owner.

Data classification is based on three objectives:

- Confidentiality
- Integrity
- Availability

There are four risks associated with each objective:

- High Risk
- Medium Risk
- Low Risk
- No Risk

Starting March 31, 2019, all State hosted data must to be classified using *Application Portfolio Management* (APM). Starting June 30, 2019, all Contractor hosted data will be classified using APM. Starting March 1, 2019 all contracts must use the Data Classification Table to assess the contracts risks. This information will be entered on the Contract MOU Review Checklist and Summary. Both the Data Classification Table and the checklist can be found on the *Templates: Technology Contracts* webpage.

Any data that is Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI), Health Information Portability and Accountability Act (HIPAA), or any information defined under State or Federal statute as confidential is automatically considered to be highly confidential. Examples risk assessments are:

- Public Assistance Records- High Risk.
- Pistol Permits Records- Medium Risk.
- Inventory of Emergency Vehicles- Low Risk.

Further information on protected information can be found in the ITSP Terms and Acronyms Directory and http://intranetbit.sd.gov/standards/PII.aspx.

All data on the State's mainframe system is automatically treated by BIT as being high risk for confidentiality, integrity and availability.

230.75.4.2. Classification of Data Produced under Contract

As part of the contract process the data owner is required to document the classification of all data produced or utilized by the project. The data classification is recorded on the Contract MOU Review Checklist and Summary provided by BIT. A copy of which will be kept by BIT and included with a copy of the contract. This includes State data that resides on a Contractor's system or data that the Contractor generates as part of a project. Also included is any State data utilized by a Contractor while providing Software as a Service (SaaS). The checklist can be found on the *Templates: Technology Contracts* webpage.

230.75.4.3. Data Classification Responsibilities

It is the data owner's responsibility to:

- Choose a systematic decision process to classify the data.
- Document the classification.
- Determine whether existing laws, regulations or agreements limit or regulate the collection, use, disclosure, access, retention and disposal of their state data. Agencies shall use all applicable published requirements, guidelines and limitations.
- Educate agency staff on the data classification procedures, requirements and guidelines.
- Based upon the results of the agency's data classification, establish data maintenance guidelines and communicate them to BIT.

- Establish a process to regularly review the appropriateness of the assigned data classifications and to adjust classifications in the event of:
    - Regulatory changes affecting an agency's management of information under its control.
    - Technologies for which data classification policies do not yet exist.

If the data is Protected Health Information (PHI) BIT recommends that the data owner perform a risk assessment as well as data classification.

It is BIT's responsibility to:

- Assure that proper access controls are implemented, monitored and audited for building, floor and/or cage access in accordance with the data classification labels assigned by the data owner.
- Submit audit results to the data owners as required by law or regulation.
- Perform regular backups of state data.
- Validate data integrity.
- Restore data from backup media.
- Fulfill the data requirements specified in agency security policies, standards and guidelines pertaining to information security and data protection.
- Retain records of data activity that include information on who accessed the data and what data was accessed as considered appropriate by the federal regulatory agency responsible for establishing security controls for the data.
- Provide appropriate security controls for contractor hosted services according to the data classification labels assigned by the data owners.

Data Center General-Access to Confidential Data-Multi-Factor Authentication

230.76.1. Overview

The implementation of Multi-Factor Authentication (MFA) improves authorization access to technology systems and enhances cyber security.

MFA provides an additional layer of protection towards the access control aspect of cyber security. MFA is an authorization technology based on at least two pieces of information. This is one additional step in the authentication process beyond the standard set of user id and passwords.

230.76.2. Purpose

The purpose of this policy is to provide direction on MFA use within State government.

230.76.3. Scope

This policy applies to remote access to the State's network.

230.76.3.1. Scope Assumptions

The usage of MFA will meet / fulfill all audit findings against the State. The solution will meet the MFA needs of protected data, equipment and sensitive applications.

230.76.3.2. Scope Constraints

This policy applies to remote access of State data, equipment, and applications.

230.76.4. Policy

230.76.4.1. Usage of Multi-Factor Authentication (MFA)

Remote access is any access to a State information system by a user communicating through an external network, for example, the Internet. MFA will be required for remote access of State data, equipment and applications.

230.76.4.2. MFA Tokens

If a user has a mobile device enrolled in the State's standard Mobile Device Management System to gain access to State resources, that mobile device is their second factor of authentication and the user will not be issued a hard token.

Mobile device authentication is the preferred method of secondary authentication.

Hard tokens are only allowed as a user's second factor of authentication if the user does not have a mobile device enrolled in the State's standard Mobile Device Management System. A user may receive and use a hard token as their alternative second factor of authentication upon approval from BIT and at the agency's expense.

Data Center General-Approved Disposal of State Data-Media Sanitization

230.77.1. Overview

There can be a significant risk when sensitive data is collected and kept on media. This media must be appropriately sanitized when no longer needed. Media sanitization methodology is dependent on the confidentiality of the data. Effective sanitization requires knowing where the data is, what the data is, and how the data needs to be protected. Any sanitation must also be checked and documented.

230.77.2. Purpose

The purpose of this policy is to ensure State data is properly sanitized when it is out of the State's control.

230.77.3. Scope

Any media containing State data in a Contractor's control. Media is any material on which data is on or may be recorded on, such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical disks. This includes both portable media and media that is installed on devices like workstations, servers, laptops, tablets, and phones.

230.77.3.1. Scope Assumptions

Electronic media with State data must be securely sanitized. The methods used are dependent on the confidentiality of the data.

230.77.3.2. Scope Constraints

Mainframe electronic media is out of scope, it has its own IRS policy requirements. Any media that is in BIT's control is also out of scope. Only media in a Contractor's control is in scope.

230.77.4. Policy

230.77.4.1. Sanitization of Media in a Contractor's Control

The required sanitization method is dependent on the data's classification, see ITSP 230.75.4.1. The data owner is responsible for classifying their data. Contractors are responsible for either sanitizing media in their care or returning it to the State as agreed to in their contract. There are two approved sanitation methods, purge or

destroy see NIST 800-88:

Purge- A method of sanitization by applying physical or logical techniques that renders target data recovery infeasible using state of the art laboratory techniques.

Destroy- A method of sanitization that renders target data recovery impossible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

Using the data security classification table which can be found on this webpage, classify the confidentiality of the data. The data's status will be based on the risks associated with the data. Any data classified as no risk does not have to be sanitized. No risk data in a contractor's care is still subject to any adverse event notification requirements agreed to in their contract.

These are the media sanitization requirements:

Low confidentiality status:

Purge

Moderate confidentiality status:

Media is not reused- Destroy Media

is reused- Purge

High confidentiality status:

Destroy

In some cases, a Contractor is legally required to keep highly confidential State data intact or otherwise cannot sanitize the data. These circumstances are dealt with in the Contractor's contract with the State. The inability to sanitize data must be included in any response to a Request for Proposals and the data owner must be informed before any contract is signed.

Following sanitization, a Certificate of Media Sanitization should be completed for each piece of media that has been sanitized, the certificate can be found on this webpage. This certificate must be sent to the State Contact who will pass it on to Data Center Director.

Data Center General-Transfer of Data-Secure Transfer of Data

230.78.1. Overview

Secure File Transfer Protocol (SFTP) is a secure version of File Transfer Protocol (FTP), which allows data access and data transfer over a Secure Shell (SSH) data stream. It is part of the SSH Protocol. This term is also known as SSH File Transfer Protocol

The SFTP makes sure data is securely transferred using a private and safe data stream. The SFTP's main purpose is to transfer data but can also be used to access an FTP server. The SFTP protocol runs on a secure channel, the client user must be authenticated by the server and no clear text passwords or file data are transferred.

230.78.2. Purpose

The purpose of this policy is to ensure that State data is securely transferred.

230.78.3. Scope

The policy covers any transfer of State data.

230.78.3.1. Scope Assumptions

This policy assumes that State data needs to be sent to or from outside the State's network or between non-State networks.

230.78.3.2. Scope Constraints

The policy does not cover non-State data.

230.78.4. Policy

230.78.4.1. Use of Secure File Transfer Protocol

SFTP must be used when State data is being sent outside the State's network, from another network to the State or is being sent between non-State networks.

Development-Application Security-Federal Tax Information

401.1.1. Overview

The acquisition, development, installation, and operation of all information systems must meet federal requirements necessary to protect Federal Tax Information (FTI).

401.1.2. Purpose

The purpose of this policy is to meet federal security requirements to safeguard FTI on any information system that is acquisitioned or developed by BIT.

401.1.3. Scope

The scope of this policy includes all information systems developed by BIT, contractors, or any third party that is involved in receiving, processing, storing, or transferring Federal Tax Information (FTI).

401.1.3.1. Scope Assumptions

This policy assumes that if the information system receives, processes, stores, or transfers FTI, it will be capable of being security scanned.

401.1.3.2. Scope Constraints

The policy only applies to information systems that receive, process, store, or transfer FTI. Security scans are not conducted on mainframe applications and desktop

applications. Due to software licensing requirements, some vendor hosted solutions do not allow for BIT to conduct security scans. Vendor hosted solutions must still comply with federal requirements to protect FTI and must meet BIT security requirements specified in contact terms.

401.1.4. Policy

401.1.4.1. Allocation of Resources and Life Cycle Support

As part of the capital planning and investment control process, BIT will determine, document, and allocate the resources required to adequately protect information systems. Security assessments will be performed as part of the Software Development Life Cycle (SDLC) process.

401.1.4.2. Information System Security Documentation

BIT will obtain, protect as required, and make available to authorized personnel, security assessment documentation for the information system. Any newly developed or acquired software, hardware, application, or website will be required to pass a security scan:

- Prior to being moved into production.
- After a significant change.
- Prior to any updates being moved into production.

A report specifying each area reviewed or audited during the assessment process will be completed and filed. The report will include all deficiencies discovered during the assessment. A solution for each deficiency will be noted and a due date for the solution to become effective will be documented. All information regarding security assessments and official records of such will be recorded in the Pegasus system.
If BIT is unable to conduct a security scan on a vendor hosted solution, the vendor must meet all security audit and vulnerability assessment requirements deemed appropriate by BIT and provide documentation of such to BIT as specified in contract terms.

401.1.4.3. Software Usage Restrictions and User Installed Software

To safeguard FTI, BIT will comply with software usage restrictions, impose and enforce limitations on user installed software on BIT workstations. Preventing unauthorized installation of non-standard software on BIT workstations and verifying that licensing requirements are met ensures that security controls implemented by BIT are not circumvented. Software and associated documentation will be used in accordance with software contract agreements and copyright laws. BIT will track the use of software and associated documentation that is protected by quantity licenses to control copying and distribution. BIT will control and document the use of peer-to-peer file sharing technology to ensure that it is not used for unauthorized distribution, display, performance, or reproduction of copyrighted work. Prior to installation on BIT workstations, open source software must go through the BIT moratorium process that includes, but is not limited to, a security assessment. Only authorized individuals are permitted to install software.

401.1.4.4. Developer Configuration Management

BIT requires that information system developers and integrators perform configuration management during information system SDLC and operation as well as manage and control changes to the information system to include:

- Documentation of approved changes to the information system and potential security impacts of the changes.
- Track security flaws and flaw resolution within the system.
- Implementation of only BIT approved changes.

Development-Application Security-Security Assessments

401.3.1. Overview

To ensure applications developed by BIT, contractors, or any third-party are protected and monitored to prevent unauthorized use, modification, disclosure, destruction, or denial of access to assets of the State.

401.3.2. Purpose

The purpose of this policy is to ensure that no hosted application, software, or website may be moved into production without passing a security assessment.

401.3.3. Scope

This policy applies to any software, application, or website developed by BIT, contractors, or by any third-party.

401.3.3.1. Scope Assumptions

This policy assumes that if the software, application, or website hosts any type of state government data, it will be capable of being security scanned. The security assessment will include active penetration testing and analysis of an application which can include, but is not limited to, the latest Top 10 categories of the OWASP (Open Web Application Security Project) and NIST (National Institute of Standards and Technology) standards.

401.3.3.2. Scope Constraints

Constraints on this policy include mainframe applications and desktop applications. Desktop applications are only scanned for connections to an unauthorized location or if it opens up dangerous ports.

401.3.4. Policy

401.3.4.1. Security Assessment

Configurations and installation parameters on all State applications must comply with BIT security management policies, procedures, and standards. All BIT developed software, third-party applications, internally hosted websites, and externally hosted websites must pass a security assessment prior to being accepted into production. The originator of the request to transfer to production will bear the responsibility of verifying that a security assessment has been performed. Written verification from the BIT Security Infrastructure Team (SIT) (BIT.ENTNETWORKSEC@state.sd.us) that the software, application, or website has passed the security assessment must be provided. Security assessments will be performed as part of the SDLC (Software Development Life Cycle) process. A security assessment of all applications supporting the needs of the Medical Management Information System (MMIS) and the Medicaid eligibility determination system will be conducted annually. For additional information on how to initiate a security assessment see 1451.5 Security Assessment Procedure.

401.3.4.2. Assessment Report

A report specifying each area reviewed or audited during the assessment process will be completed and filed. To view the report form, see Audit findings template follow up. The reports shall be reviewed by the BIT SIT on a quarterly basis to ensure all deficiencies have been resolved in a timely manner.

401.3.4.3. Annual Review

BIT will form an annual assessment team comprised of individuals who have been identified as having the knowledge and skills to properly assess the requirements for security controls, assessing risk, and understanding the various user needs of the system. These individuals shall also understand the consequences of non- adherence to security controls and processes. The BIT assessment team will conduct an annual assessment of security controls for applications and systems. This assessment will be performed concurrently with annual security discussions and will verify:

- The extent to which security controls are implemented correctly.
- Security controls are operating as intended.

- Security controls meet the life cycle and level of risk security requirements of the applications, websites, software, and systems.

Development-Application Security-Data Encryption

401.5.1. Overview

This policy covers rules for storing sensitive data used by applications and systems.

401.5.2. Purpose

The purpose of this policy is to outline what encryption algorithms and encryption tools are approved to use to encrypt columns in the State databases. The policy defines the minimum level of data that is required to be encrypted.

401.5.3. Scope

All data required to be encrypted must comply with this policy by June 30, 2024.

401.5.3.1. Scope Assumptions

This policy does not apply to Mainframe systems. Mainframe data is encrypted at rest which complies with IRS 1075.

401.5.3.2. Scope Constraints

This policy applies to applications and/or systems that have been developed or rewritten by BIT, contractors employed by BIT, and/or third-party vendors contracted by the State.

401.5.4. Policy

401.5.4.1. Data Encryption

All High Impact Personally Identifiable Information (PII) Data is required to be encrypted at both at rest and in transit. High Impact PII includes, but is not limited to, Social Security Numbers (SSNs), Federal Tax Information (FTI), and Protected Health Information (PHI). See BIT PII Storage Standards http://intranetbit.sd.gov/standards/PIIstorage.aspx. Other data may be recommended or required to be encrypted depending on the results of Software Development Life Cycle (SDLC) security reviews.

401.5.4.2. Hashing Values

Only values that are not going to be decrypted can use a hashing algorithm, all other values must use one of the encryption tools or algorithms listed above. Data that cannot be hashed includes, but is not limited to, Protected Health Information (PHI), Federal Tax Information (FTI), and Personally Identifiable Information (PII).

401.5.4.3. Tools

See BIT PII Storage Standards http://intranetbit.sd.gov/standards/PIIstorage.aspx for the acceptable Tools for encryption.

401.5.4.4. Compliance Measurements

The BIT Development Enterprise Team will verify compliance to this policy through various methods including, but not limited to, business tool reports, and internal and external audits.

401.5.4.5. Exceptions

Any exceptions to this policy must be approved in advance by the BIT Development Enterprise Team Manager.

401.5.4.6. Non-Compliance

Applications that do not meet the requirements of this policy will not be permitted into a production environment until the requirements of this policy have been satisfied.

Development-Application Security-Authentication and Authorization

401.7.1. Overview

This policy defines how authentication and authorization is implemented on websites, applications, and systems for the protection of State data.

401.7.2. Purpose

The purpose of this policy is to set the minimum requirements for how to work with and create applications, websites, and systems that require user authentication and role-based authorization of users.

401.7.3. Scope

This policy applies to all new applications, websites, and system rewrites.

401.7.3.1. Scope Assumptions

The applications, websites, or systems referred to in this policy include new development and those being rewritten. Any application, website, or system that receives, possesses, stores, or transfers Federal Tax Information (FTI) must follow the policy sections for FTI.

401.7.3.2. Scope Constraints

The applications, websites, or systems referred to in this policy must have been developed or rewritten by the Development division of BIT, contractors employed by BIT, and/or third-party vendors contracted by the State. This policy does not apply to applications or websites hosted by contractors or third-party vendors.

401.7.4. Policy

401.7.4.1. User Authentication and Authorization

If your project uses authentication and authorization of users with different roles it must include the following requirements.

- Web applications for sd.gov services that require a logon screen for user authentication must use mySD single sign on (SSO) authentication.

- Desktop applications that require user authentication functionality must use Active Directory or SSO for logon and role management, if possible.
- Mainframe systems that require user authentication functionality must use Resource Access Control Facility (RACF).
- Shared use of User Accounts is not permitted. When user accounts are created, they must be created for an individual - not for a group.

If custom authentication is required, it must be approved before the project begins, unless an exception has already been granted.

401.7.4.2. Password Requirements

The following password requirements must be built into your project.

1. Enforce a minimum password complexity of:
   - Eight-character minimum and a maximum of 64 characters.
   - At least one numeric and at least one special character.
   - A mixture of at least one uppercase and at least one lowercase letter.
   - Storing and transmitting only encrypted representations of passwords.
2. Enforce password minimum lifetime restriction of one day
3. Prohibit Password reuse for 24 generations
4. Allow the use of a temporary password for system logon requiring an immediate change to a permanent password
5. Password-protect system initialization (boot) settings
6. Allow passwords to be copied and pasted into the login.
7. No passwords hint.
8. No knowledge-based authentication. (For example, what was the name of your first pet?).

If your project involves FTI it must include the following requirements, in addition to those listed above.

- Enforce non-privileged account passwords to be changed at least every 90 days.
- Enforce privileged account passwords to be changed at least every 60 days.

401.7.4.3. Invalid Login Attempts for projects using Federal Tax Information

If your project involves FTI, it must include the following requirements.

- Enforce a limit of three consecutive invalid login attempts by a user during a 120-minute period by automatically locking the account for a period of at least 15 minutes.
- Prevent further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user.
- Retain the session lock until the user reestablishes access using established identification and authentication procedures.
- The information system must automatically terminate a user session after 30 minutes of inactivity.

401.7.4.4. reCAPTCHA

ReCAPTCHA will be required on all login pages and public facing form submissions unless they are protected by a login page that already uses reCAPTCHA. For more details on how to implement reCAPTCHA, see Procedure 1451.3.

401.7.4.5. Tools

For instructions on how to use mySD in your application, visit mySD.sd.gov and click Developer Toolkits.

401.7.4.6. Compliance Measurements

The BIT Development Enterprise Team will verify compliance to this policy through various methods including, but not limited to business tool reports and internal and external audits.

401.7.4.7. Exceptions

Any exceptions to this policy must first be approved in advance by the Development Enterprise Team Manager.

401.7.4.8. Non-Compliance

Projects that do not meet the requirements of this policy will be subject to additional development to add the required functionality listed in this policy to the project before it will be permitted into a production environment.

Network-Service-Access Control

610.1.1. Overview

Access to the technology infrastructure of the State is essential to maintaining a productive workforce. With this access comes the risk and responsibility of approving, monitoring, and securing the users, workstations, and systems being accessed to protect their confidentiality, integrity, and availability. Controlling access to State technology systems is paramount to avoid damages. Such damages include loss of sensitive or confidential data, destruction or theft of intellectual property, harm to public image, disruption of or damage to public safety activities, and fines or financial liabilities incurred as a result of the damage.

610.1.2. Purpose

The purpose of this policy is to establish rules, guidelines and expectations surrounding access to State technology resources.

610.1.3. Scope

BIT is responsible for designing, configuring and maintaining access to technology systems owned by or operated for the State and its citizens. To supply reliable and secure access, standards and policies for limiting and controlling technology access are established in this policy.

- All State employees and contractors with a State-owned or non-State-owned workstation used to connect to the State network or State infrastructure;
- Remote access connections, to include but not limited to the Internet, used to complete tasks on behalf of the State, including email access and viewing Intranet resources;
- All workstations and devices utilized, and the technical implementations of access used to connect to State networks;
- Communication - originating from and to - DDN Intranet and DMZ.

610.1.3.1. Scope Assumptions

BIT has standardized access control methods and technologies. Only users, workstations, accounts and services compliant with or outlined in this policy are permitted within the DDN. An Agency specific clause is documented in the policy section. The policy applies to the Department of Social Services systems and applications referenced. The policy assumes that Department of Social Services systems and applications referenced are supported or maintained by developers and support staff who have access to remote connections.

610.1.3.2. Scope Constraints

While this policy applies to BIT managed technology systems at our K-12 and Higher Education client locations, this policy does not apply to users and workstations managed and operated by those institutions on their local networks.

610.1.4. Policy

610.1.4.1. System Access Expectations

All access for user and/or system level rights must be granted, reviewed and approved by BIT for accuracy and adequacy to ensure that the appropriate level of access for the intended functions is granted. All access methods utilized to connect to State networks must be implemented through approved combinations of hardware and software security tools that have:

- Unique identification or UID for each user.
- System level identification for each system (e.g. Active Directory accounts).
- Capability to restrict access to specific nodes or network applications.
- Access control software or hardware that protects stored data and the security system from tampering. Audit trails of successful and unsuccessful log-in/access attempts.
- Account credentials must not be stored in unencrypted fashion on any workstation or storage platform.

If a system requires access control methods that fall outside of the listed requirements, the agency sponsoring or requesting that system must work with their BIT Point of Contact to engage BIT in a review of this system. If an exemption would be required, the *Security Exemption Request Form* at the BIT Intranet (http://intranet.bit.sd.gov/forms) must be submitted to the BIT HELP Desk (773-4357) for exemption considerations. Unrestricted access into or out of the DDN Intranet and/or DMZ is prohibited. Systems or applications that must call out to a remote system or "call home" for any reason must be vetted and approved by BIT prior to their installation within State infrastructure.

610.1.4.2. Contractor Access

Access to the DDN Intranet and DMZ by contractors is rigorously controlled and managed. The following rules apply to any contractors connecting to State infrastructure:

- Requests for contractor access to technology infrastructure must be approved by BIT. A *Security Exemption Form*, located at the BIT Intranet (http://intranet.bit.sd.gov/forms), submitted to the BIT HELP Desk (773-4357) is required to gain any level of access to State technology systems.
- Contractor access will be limited to the bare-minimum number of systems necessary to accomplish BIT- approved tasks and procedures. This access will be controlled by any number of mechanisms, to include, but not limited to, user accounts, firewall policies, Group Policy, scheduled lockdown and maintenance windows, and/or Skype for Business remote access with BIT personnel monitoring and controlling the access.
- Contractors will not have any access to State workstations without explicit authorization from the BIT Commissioner or BIT Chief Information Security Officer. A *Security Exemption Form*, located at the BIT Intranet (http://intranet.bit.sd.gov/forms), submitted to the BIT HELP Desk (773-4357) is required to request access.
- Administrative accounts on State technology systems must be fully vetted by BIT, periodically reviewed for accuracy and necessity, and limited to the minimum level of systems and access necessary. Domain, enterprise, or similar administrative access levels are strictly prohibited for contractors.

610.1.4.3. Modems

Dial-in or dial-out telephony modems are not allowed to be connected to servers or any other technical assets of the State for any use. Digital Subscription Lines (DSL), cellular and cable modems managed by BIT are not considered telephony modems under this policy.

610.1.4.4. Remote Access

Remote access to the DDN Intranet and DMZ, to include all data files and applications, must be BIT managed, secured and encrypted. Any remote access where Federal Tax Information (FTI) and or Criminal Justice Information System (CJIS) data is accessed over the remote connection must be performed using multi-factor authentication. Supported forms for remote access are:

- Secure Sockets Layer (SSL) - an Internet Web Browser with a minimum of 256-bit encryption.
- CSG - the Citrix Secure Gateway of the State.

- NetMotion - a VPN client maintained by BIT.
- Horizon View (VDI).
- Skype for Business - a collaboration system operated by BIT, can be used if and only if a BIT staffer monitors and manages the access during all remote access sessions.

SSL VPNs are not permitted under any circumstances. There is no direct remote access using Remote Desktop Protocol (RDP) allowed from the Internet to the State network or to any cloud-based resource with access to the State network. Indirect RDP access from the Internet is only allowed if it goes through a BIT-approved remote access service.

610.1.4.5. Inspection and Review

BIT will verify compliance to this policy through a number of methods, including but not limited to: periodic walk- throughs, video monitoring, internal and external audits, automated systems processes, business tool reports, and inspections. Feedback will be provided to the required entities.

610.1.4.6. Department of Social Services

In November of each year, a review will be conducted of all personnel with remote access to a major system supporting the needs of the Medicaid Management Information System (MMIS).

- A document will be generated and filed containing the names of personnel with remote access and privileged functions.
- If a determination is made that an individual no longer requires remote access to MMIS, then the remote access will be terminated.

In November of each year, a review will be conducted of all personnel with remote access to a major system supporting the needs of the Division of Child Support.

- A document will be generated and filed containing the names of personnel with remote access and privileged functions.
- If a determination is made that an individual no longer requires remote access to the Division of Child Support System, then the remote access will be terminated.

Network-Concept-Security Domain Zones

610.3.1. Overview

All devices connected to any technology infrastructure of the State must be protected. The connections must be designed and implemented to ensure compliance with the access control policies for each connected system.

610.3.2. Purpose

Different areas or zones of the State network require different levels of protection and security. This policy will define the different zones and expectations for each zone.

610.3.3. Scope

Links to external networks, including but necessarily not limited to, the Internet, federal agencies, and third-party companies must be managed by BIT to ensure the security of the technology infrastructure of the State.

610.3.3.1. Scope Assumptions

All individuals that utilize the DDN must work with BIT to define business practices or align connectivity into one of the three security domain zones which are the Intranet Zone, De-Militarized Zone (DMZ), and Extranet Zone. BIT will not always be able to allow devices and assets to communicate amongst the Security Domain Zones for security reasons, which can include Federal requirements.

610.3.3.2. Scope Constraints

Networks outside of the control of BIT, such as the local university networks operated by Higher Education are outside of the scope of this policy.

610.3.4. Policy

610.3.4.1. Intranet

The Intranet zone is the private, internal network that contains traditional clients of the State and internal business systems. To access the Intranet from external locations, such as the Public Internet, a *Firewall Modification Request Form* must be completed at the BIT Intranet (http://intranet.bit.sd.gov/forms). Only approved methods and technologies can be used to traverse into the Intranet from other network zones.

610.3.4.2. DMZ

The DMZ is the portion of the DDN that provides limited security services and is designed to support services and systems that are utilized by external users. In most situations, the external users require access to resources in the DMZ from the Public Internet. All services and systems that need to be publicly accessible must be placed within the DMZ zone. Access to the DMZ from external locations will require an approved *Firewall Modification Request* Form completed at the BIT Intranet (http://intranet.bit.sd.gov/forms).

610.3.4.3. Extranet

The Extranet zone is segmented from the Intranet zone and the DMZ zone to support network connections for agencies that are not part of the infrastructure of the State Intranet due to business situations. Access to the Extranet from external locations will require an approved *Firewall Modification Request Form* completed at the BIT Intranet (http://intranet.bit.sd.gov/forms).

Network-Concept-Network Integrity

610.9.1. Overview

The DDN is a complex network containing a multitude of inter-dependent systems, connections, and roles. Adequate security measures must be in place to protect the technical assets of the State - physically and logically
- from damage, theft, vandalism, and other forms of threats to maintain the integrity of the network.

610.9.2. Purpose

This policy is to establish the baselines of how network integrity is maintained through technology standards and personnel practices. Adequate security measures must be in place through these standards to protect the technical assets of the State.

610.9.3. Scope

Technologies, contracts, and practices, to include hardware, software or circuits, must be physically and logically protected against theft, damage, and misuse.

610.9.3.1. Scope Assumptions

By maintaining accurate accountability of property and instituting appropriate countermeasures to safeguard property, the opportunity for loss, theft or pilferage of valuable technical resources can be greatly diminished. Clients that request the construction of a local or wide area network will work with BIT for the design, implementation, and support matrix of the proposed network segment.

610.9.3.2. Scope Constraints

While this policy applies to BIT managed equipment at BIT's higher education client locations, this policy does not include the private, internal networks of BIT's higher education clients.

610.9.4. Policy

610.9.4.1. Responsibilities

BIT is responsible for providing secure and reliable network connectivity through approved and managed platforms for agencies. This responsibility encompasses local networks, wide-area networks, wireless networks, cellular networks, secure remote access networks, and relevant security components.

610.9.4.2. Management

BIT will manage network connectivity platforms for agencies. This responsibility encompasses local networks, wide-area networks, wireless networks, cellular networks, secure remote access networks, and relevant security components.

610.9.4.3. Disabling Critical Components of Network Security Infrastructure

Critical components of the BIT network security infrastructure must not be disabled, bypassed or turned off without prior approval from the Director of the Division of Telecommunications or their designee(s).

610.9.4.4. Technical Asset or Contractor Connections

Connection of any contractor and/or their equipment to the DDN or any subsystem requires prior approval from the BIT Commissioner or their designee(s). To request any equipment to be installed or connected to the DDN, requestors will begin by submitting a request to the BIT HELP Desk (773-4357) and must provide two weeks' notice. The request must include the dates, times, duration of connection, and the reasons for the connectivity. The requestor must be ready to provide the technical device, any available documentation, and technical contacts to BIT.

610.9.4.5. Local Area Network

All LANs must follow the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard for wired Ethernet networks. State wireless networks operate only in accordance to the wireless policy. Devices and systems in use must meet the specifications laid out by IEEE, to include but not necessarily limited to: 802.1x, 802.3x full duplex, 802.3, 802.3z 1000BASE-LX, 802.3ab 1000BASE-T, 802.3z 1000BASE-X, 802.3ae 10GbE LAN-PHY, 802.1w
RSTP, 802.1s, 802.3ad with LACP support, 802.1Q.Wired network ports that are not individually identified as in use by a State employee, such as those in conference

rooms or public areas, will remain disabled unless specifically requested via the BIT HELP Desk (773-4357). Requests must include the dates and times these ports will be used by State employees.

610.9.4.6. Wide Area Network

To assure privacy through carrier networks, all carrier-based services utilize private virtual links in a fashion determined and maintained by BIT. This can include, but is not necessarily limited to, carrier managed Multiprotocol Label Switching (MPLS) networks, Metro Ethernet (MEF) networks, dark fiber networks, or IPSec secured virtual private networks (VPNs) over commercial Internet services. Secure socket layer (SSL) VPNs are not allowed in any location on the network.

610.9.4.7. Physical Controls

All line junction points to include cable and line facilities must be located in secure areas or an area that is locked with a key or similar allowed system. Devices to include but not limited to firewalls, servers, switches, hubs, routers, and wireless access points, must be protected from unauthorized physical access.

Network-Communication-Internet

610.11.1. Overview

All devices connected to any technology infrastructure of the State must be protected. BIT is responsible for defining and managing the method, services, and providers used to access the Internet. The Internet is a tremendous tool to be utilized by the State, but the open-system architecture of the Internet creates risks that must be mitigated; BIT does not control the Internet. All Internet access to or originating from the DDN must be approved through the BIT HELP Desk (773-4357).

610.11.2. Purpose

Access to and access from the Internet is approved, managed, and maintained by BIT.

610.11.3. Scope

This policy establishes acceptable expectations for connections from a State office or connected entity to the public Internet. It establishes rules and regulations for the types of, ownership of, and equipment involved in public Internet connections and the DDN.

610.11.3.1. Scope Assumptions

Devices or networks connected to the DDN are expected to comply with this policy.

610.11.3.2. Scope Constraints

Networks not fully under the management of BIT, such as the local county government networks in a courthouse, are out of scope for this policy.

610.11.4. Policy

610.11.4.1. Multiple Connections

No entity or device that participates on the DDN may maintain or install an Internet connection on a network that is also connected to the DDN. Devices are not permitted to be dual-homed (connected to the DDN and the public Internet simultaneously). All traffic destined to the Internet from a DDN-connected entity or arriving from the Internet to the DDN must be through BIT managed solutions. K-12 schools or Post-Secondary Educational institutions that are connected to the DDN are not allowed to have a connection to a public ISP.

610.11.4.2. Interfaces

Establishing a direct, real-time connection between the DDN and external organizations networks, such as Federal Government, contractor support, or any other public or private network, must be approved by BIT. Additional tasks may be required from BIT to determine what additional suitable security measures can be implemented for the connection. All real-time, external connections to the technology infrastructure of the State must pass through a firewall or a similar technology entry point.

610.11.4.3. Security

Only services that are explicitly authorized by BIT will be permitted inbound and outbound between the DDN Intranet and the Internet. BIT is responsible for periodically reviewing the implemented security rules for devices that manage inbound and outbound connections. Depending on vulnerabilities and other security risks identified, access to the Internet and from the Internet to the DDN can be restricted and/or expanded without notice.
Individuals may not probe security mechanisms at any DDN site, State facility or Internet location without specific, written permission that has been obtained from an authoritative person from each of the affected entities.
Similarly, any scanning or security probing activity against a DDN site or State facility requires written permission from the BIT Chief Information Security Officer before such an activity is performed. Unauthorized behavior will be referred to the appropriate law enforcement agency.

610.11.4.4. Responsibilities

Devices connected to the DDN may not be used to make unauthorized connections, to break into, or adversely affect the performance of any asset on the DDN or the Internet. All equipment of the State, including but not limited to, workstations, email system, Internet access tools, and other information systems, are restricted to official State business use only.

610.11.4.5. IPv4/IPv6 and Device Names

BIT is responsible for the management of the DDN public IPv4/IPv6 address space which has components used by the State to include the assignment of device names. Workstations and servers are required to use Dynamic Host Configuration Protocol (DHCP) for the assignment of IPv4/IPv6 addresses. Requests for an exemption from DHCP must be submitted to the BIT HELP Desk (773-4357) for review using the *Security Exemption Request Form* at the BIT Intranet (http://intranet.bit.sd.gov/forms). For application access, applications are prohibited from using individual IPv4/IPv6 addresses. Domain names must be created for application reference instead of IPv4/IPv6 address. Requests for an exemption from references to domain names must be submitted to the BIT HELP Desk (773-4357) for review using the *Security Exemption Request Form* at the BIT Intranet (http://intranet.bit.sd.gov/forms). If an exemption is granted, the requestor assumes all liability for the support and the maintenance of the application when the host address is required to change due to infrastructure changes on the DDN. IPv4/IPv6 Addresses and device names are considered classified, private information of the State.
Naming standards and IPv4/IPv6 addresses for workstations, servers, networking equipment, security devices, and any other technical device are classified as protected, nonpublic information that may not be distributed without express, written approval of the BIT Commissioner to an entity not associated with the State. Other internal network addresses, identifiers, configurations, and related system design information for the technology infrastructure of the State must be restricted. Technical devices and users outside the DDN must be unable to access classified information without explicit management approval. Exemptions to information access must be submitted to the BIT HELP Desk (773-4357) using the *Security Exemption Request Form* at the BIT Intranet (http://intranet.bit.sd.gov/forms).

Security-Network Discovery-Probing-Exploiting

620.1.1. Overview

BIT establishes and maintains security controls to secure State devices and protect data; therefore, it is important to provide guidelines to strictly prohibit individuals from probing the DDN network, including network, service and port discovery, or trying to exploit these security controls that exist on the DDN.

620.1.2. Purpose

This policy is designed to provide clarification on Probing/Exploiting Security Controls.

620.1.3. Scope

This policy provides a baseline set of expectations for security policies as applied to the State information technology systems.

620.1.3.1. Scope Assumptions

Security controls are tested frequently throughout the State infrastructure. This includes testing all BIT managed devices; external devices that require connectivity, including contractors and other unmanaged connections; workstations used by K-12 and Higher Education.

620.1.3.2. Scope Constraints

While this policy applies to BIT managed devices and users at our K-12 and Higher Education client locations, it does not apply to the local devices and networks operated by those institutions.

620.1.4. Policy

620.1.4.1. Limiting Tool Functionality

Technical tools must be used as directed by the manufacturer or BIT. Utilizing technical tools to cause damage to devices or disrupting the desired data flow across the DDN is prohibited. Authorization to use software such as packet capture, network probing, and network and endpoint discovery tools for troubleshooting activities does not imply that consent has been provided to utilize these tools without limitations. Individuals, identified in name, by the Director of the Division of Telecommunications are permitted to use discretion to expand the functionality of technical tools.

620.1.4.2. Exploiting Security Controls of Information Systems

All individuals must not exploit vulnerabilities or deficiencies found in information systems or perform probing of State network devices to damage systems or data. It is not permitted to obtain information that the individual is not authorized to view, to take resources away from other individuals, or to gain access to other systems for which proper authorization has not been granted. Any exploitation of vulnerabilities in information systems and damage from scanning or probing found must be reported using the Detailed Incident form located on the BIT Intranet.

620.1.4.3. Cracking Application or Passwords

All individuals are strictly prohibited from "cracking" passwords of the technical assets that exist on the DDN. Exemptions must be approved, in advance, and in writing, by the BIT Chief Security Information Officer. The *Security Exemption Request Form* at the BIT Intranet (http://intranet.bit.sd.gov/forms) must be used to request an exemption. Individuals, identified in name, by the Director of the Division of Telecommunications are permitted to "crack" passwords.

620.1.4.4. Exemptions

Exemptions must be approved, in advance, and in writing, by the BIT Chief Information Security Officer. Activities that are prohibited include but are not limited to the use of scanning software and utilities, keylogging devices, vulnerability assessment tools, and denial-of-service utilities. Exemptions for probing and exploiting security controls must be submitted to the BIT HELP Desk (773-4357) by using the *Security Exemption Request Form* at the BIT Intranet (http://intranet.bit.sd.gov/forms).

Security-Content Control-Internet Filtering

620.5.1. Overview

All content accessed from the DDN must be sufficiently protected and monitored to be consistent with BIT Information Technology Security policies. These policies are designed to prevent unauthorized use, modification, disclosure, destruction or denial of access to State assets. Therefore, Internet traffic is monitored for all users and workstations connected to the DDN Intranet. Domain administrative accounts are prohibited from browsing the Internet.

620.5.2. Purpose

Primary purpose is to protect and secure information and assets managed by the State. Secondary purpose is to inform and educate users of their responsibilities towards the use of information, products, and services obtained from the Internet.

620.5.3. Scope

This policy incorporates all users initiating communication between workstations connected to the DDN and the Internet, including web browsing, (IM) instant messaging, file transfer, file sharing and the Intranet.

620.5.3.1. Scope Assumptions

Content filtering is provided to all users to protect them from the unintentional or deliberate accessing of Internet content that is offensive and inappropriate. Employees, contractors, and devices connected to the DDN must adhere to this policy.

620.5.3.2. Scope Constraints

This policy does not apply to K-12 and Higher Education accounts with administrator privileges. While this policy applies to BIT managed devices and users at our K-12 and Higher Education client locations, it does not apply to the local devices operated by those institutions.

620.5.4. Policy

620.5.4.1. Exemptions

If requesting a filter exemption, then justification is required. Exemptions to this policy must be submitted to BIT via the *Security Exemption Request Form* at the BIT Intranet (http://intranet.bit.sd.gov/forms). BIT will review the impact to the technology infrastructure of the State for each requested exemption; the period for the review process should not exceed two weeks. Exemption Details:

- All Internet filtering exemptions must be approved by the BIT Commissioner.
- All requests for the data of an individual pertaining to Internet practices must come from the Department Secretary or Bureau Commissioner of the agency directly to the BIT Commissioner as requests for data are handled at the highest level possible.
- A report on an individual should be completed within two weeks. All requests for data must be approved by the BIT Commissioner.

620.5.4.2. Appropriate Use of Administrator Access

Accounts that are members of the SD Domain Administrators group have administrator access to Active Directory services and systems. Use of those accounts specific to Internet access is strictly prohibited. These include Administrators, Domain Administrators, and other accounts with a level of access beyond that of a normal user account. Use of these privileged accounts is restricted to administrative responsibilities and must be prohibited from non-administrative activities. Web browsing or any access to/from the Internet under an Administrator role is strictly prohibited. A malicious website can be used to compromise a workstation or server while online. A

compromised asset with elevated Administrative privileges can cause significant additional harm over that of a normal user account.

620.5.4.3. DDN Content Filtering

BIT does not manage filtering of any degree for K-12 schools. BIT does not manage content filtering of any degree for Higher Education facilities. K-12 and Higher Education are completely responsible for the content that is permitted or blocked for their institutions.

620.5.4.4. DDN Intranet Content Filtering

BIT policy shall block access to the following categories, based on standard Web filtering suggestions. These categories are deemed inappropriate:

- Adult/Sexually Explicit Material
- Gambling
- Hacking
- Illegal Drugs
- Personals and Dating
- Malicious Websites
- Phishing
- Tasteless and Offensive Content
- Violence, Intolerance, and Hate
- Weapons
- Web Based Email
- Peer to Peer (P2P) File Sharing

620.5.4.5. Filter Exemption Requests

If access to a blocked Internet site is necessary for reasons related to work expectations or data is needed to understand the Internet surfing habits of an individual, the Department Secretary, Bureau Commissioner, or Executive Leadership must submit a request directly to the BIT Commissioner through the BIT HELP Desk (773- 4357). Requests related to Internet site administration for the individual to meet work expectations or individual investigations are handled at the highest management level possible. Requests for access to blocked sites and requests for information on surfing habits are documented in the work order system maintained by the BIT HELP Desk (773-4357). The content-filtering category database of the filtering solution is updated daily. Requests must include:

- The name(s) of the requestor.
- The phone number(s) of the requestor.
- The SD Domain UID(s) of the requestor;
- The site for which access is required or the scope of the data requested for an individual.
- The length of time required for access to the site or the time-period to be recorded in a report.

TERMS

Abstraction Technologies
The removal of the network control and forwarding functions that allows the network control to become directly programmable and the underlying infrastructure to be separated for applications and network services. *See also Directory, IP Address, and Relative Pathing.*

Access Attempts
When a user tries but fails to connect to an application or database so that they can make use of the resource.

Accreditation (also referred to as Vulnerability Assessment)
Scanning of a system looking for security vulnerabilities.

Accreditation Boundary
All components of an information system to be accredited by an authorizing official and excludes separately accredited systems to which the information system is connected. If a set of information resources is identified as an information system, the resources should:

- Generally, be under the same direct management control.
- Have the same function or mission objective and essentially the same operating characteristics and security needs.
- Reside in the same general operating environment (or in the case of a distributed information system, reside in various locations with similar operating environments.)

ADABAS
Software AG's database management system (DBMS). ADABAS organizes and accesses data according to relationships among data fields. The relationships among data fields are expressed by ADABAS files, which consist of data fields and logical records.

Ad hoc Networking (WANET or MANET)
A decentralized type of wireless network, considered ad hoc because it does not rely on a pre-existing infrastructure, such as routers or access points.

Adverse Event
An observable occurrence where there is unauthorized use of system privileges, unauthorized access to State data, execution of malware, physical intrusions, or electronic intrusions that may include network, applications, servers, workstations, and social engineering of staff.

Agency
An association, authority, board, commission, committee, council, department, division, task force or office within the Executive Branch of State government. Includes the staff of that individual department.

Application
A complete and self-contained program or group of programs designed to perform a function for the user.

Application Scans
Scans performed by BIT against business software applications to identify security vulnerabilities. This includes applications BIT writes and software that is procured from other software companies.

Application Server
A type of server designed to install, either on workstations or other servers, operate, host applications, and associated services for end users and I/T services. It facilitates the hosting and delivery of applications, which are used by multiple and simultaneously connected local or remote users.

Authorized Developer
An individual which has been granted permission and access to systems by an administrator of said system so that they can build and create software and applications.

Authorized Persons
The vendor's and their employees, contractors, subcontractors, or other agents who need and have been granted access to the State's data or IT facilities to enable the Vendor to perform the services required.

Back Door
Access to a computer program that bypasses security mechanisms. A programmer may sometimes install a back door so that the program can be accessed for troubleshooting or other purposes during development.
Attackers can use back doors that they detect, or install themselves, to gain access to an application or database for malicious purposes.

Blocked mail
Incoming emails which are being stopped at the mail gateway because they are or appear to be phishing emails, spam, or they have malicious attachments.

Bluetooth
The wireless communication technology that conforms to the Bluetooth computing and telecommunications industry specification. This specification describes how mobile phone, landline phones, computers, and mobile devices can easily exchange information by using a short-range wireless connection.

Browser
A software application used to locate, retrieve, and display content from the World Wide Web, including Web pages, images, video, and other files.

Brute Force Attack
A hacker sets up an automated process against login pages to repeatedly test the user id or password. If they guess a correct combination, they have gained access to the system.

Bureau of Information and Telecommunications
The Bureau of Information and Telecommunications which strives to partner and collaborate with clients in support of

their missions through innovative information technology consulting, systems, and solutions.

Business Associate (BA)
A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity or another Business Associate. Business associate functions and activities include: claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing. Business associate services are: legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial. BIT is considered a Business Associate of DSS, DOH, DHS, and BHR.

Business Associate Agreement (BAA)
An agreement with a third party or vendor to assure the State that the vendor is appropriately protecting confidential client information and data. If a governmental agency is the BA of another governmental agency who is the covered entity a MOU maybe substituted for a BAA. See also Regulated data and Health Information Portability and Accountability Act.

Chief Information Security Officer (CISO)
BIT senior executive charged with implementing the information technology security programs for the State.

Circuit
A theoretical structure simulating electrical and data paths.

Closed Source
Proprietary software where the state does not hold the copyright.

Cloud Service
Services made available to users on demand via the internet from a cloud computing provider's server as opposed to being provided by the State's on-premise servers. *See also Infrastructure as a Service and Platform as a Service.*

Code
The instructions commonly used in a program that cause a computer to perform a specific task.

Commercial off the Shelf Software
Closed source software that is purchased and used by the State with no changes made by the vendor.

Communication Protocols
The agreed upon format for data that allows the data to be sent between computers.

Connectivity
The ability of hardware devices or software packages to transmit data between other devices or packages.

Content Filtering
Using a program to screen and exclude from access or availability, Web pages or email that is deemed objectionable.

Contractor
Regarding a signatory to a contract or agreement, the terms Contractor, Consultant, and Vendor are equivalent. Subcontractors, Agents, Assigns and/or Affiliated Entities are not signatories to the contract or agreement. The ITSP may be attached to the contract or agreement and all policies in the ITSP apply to all.

Covered Entity
A HIPAA covered entity is any organization or corporation that directly handles Personal Health Information (PHI) or Personal Health Records (PHR). The most common examples of covered entities include hospitals, doctors' offices, and health insurance providers. DSS, DOH, and BHR are covered entities. *See also Business Associate, Regulated data and Health Information Portability and Accountability Act.*

Cracking passwords
The process of recovering passwords from data that have been stored in or transmitted by a computer system.

Credentials
Credentials are a UID plus additional information and data such as a password, account number, or access code.
Examples are:
- RACF
- NATURAL

Data and Information Types
Data is measured, collected, reported, and analyzed. Data as a general concept refers to the fact that some existing information or knowledge is represented or coded in some form suitable for better usage or processing. Pieces of data are individual pieces of information.

Data and Information Types: Confidential
Any data or information, other than trade secrets, that is materially sensitive in nature, whether manual or electronic, which is valuable and not generally known to the public. Identified here, are few examples, this list is not inclusive. Personally Identifiable Information which is not in the public domain, and if improperly disclosed could be used to steal the identity of an individual, violate the right of an individual to privacy or otherwise harm the individual or business to include, but is not limited to social security numbers, tax payer identification numbers, and any other department determined data that is not in the public domain or intended for release to the public domain and if improperly disclosed might:
- Cause a significant or severe degradation in mission capability.
- Cause loss of organizational integrity or public confidence.
- Result in significant or major damage to organizational assets.

- Damage the integrity of the State.
- Result in significant or major financial loss.
- Result in significant, severe, or catastrophic harm to individuals.

Data and Information Types: Federal Tax Information (FTI)
Consists of returns or return information and may contain personally identifiable information (PII). FTI is any return or return information and data received from the Internal Revenue Service (IRS) or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service. FTI includes any information created by the recipient that is derived from return or return information and data. FTI does not include information and data provided directly by the taxpayer or third parties. If the taxpayer or third party subsequently provides returns, return information and data or other PII independently, the information and data is not FTI as long as the IRS source information and data is replaced with the newly provided information and data.

Data and Information Types: Personally Identifiable Information (PII)
Any information about an individual that is maintained or collected by an agency, including:
- Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.
- Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Data and Information Types: Protected
Very specific types of data regulated by law, which includes but is not limited to PCI, FERPA, HIPAA, GLBA, ITAR and EAR.
- FERPA: Education records are protected by FERPA (Family Educational Rights and Privacy Act). For example, tax records of parents and students, class lists, grade rosters, records of advising sessions, grades, and financial aid applications.
- HIPAA: Certain health information and data is protected by HIPAA (Health Information Portability and Accountability Act) if it is individually identifiable and held or transmitted by a covered entity. For example, health records, patient treatment information and data, health insurance billing information and data.
- GLBA: Financial records are protected by GLBA (Gramm-Leach Bliley Financial Services Modernization Act).
- ITAR and EAR: Export Controlled Research is protected by ITAR (International Traffic in Arms Regulations) and EAR (Export Administration Regulations). For example, dual-use technology used for scientific advancement as well as military applications, see SDCL 1-27-1.5

Data and Information Types: Return Information
Any information and data collected, or generated, by the IRS with regard to any person's liability, or possible liability, under the Internal Revenue Code (IRC). Return information and data includes, but is not limited to:
- Information and data, including the return, that IRS obtained from any source or developed through any means that relates to the potential liability of any person under the IRC for any tax, penalty, interest, fine, forfeiture, or other imposition or offense;
- Information and data extracted from a return, including names of dependents or the location of business, the taxpayer's name, address, and identification number. Information and data collected by the IRS about any person's tax affairs, even if identifiers, such as name, address, and identification number are deleted. FTI may include PII. FTI may include the following PII elements:
- The name of a person with respect to whom a return is filed
- His or her mailing address
- His or her taxpayer identification number
- Email addresses
- Telephone numbers
- Social Security Numbers
- Bank account numbers
- Date and place of birth
- Mother's maiden name
- Biometric data (e.g., height, weight, eye color, fingerprints)
- Any combination of the preceding.

Returns are forms submitted on paper or electronically with return information to the IRS by, or on behalf of, or with respect to any person or entity. Examples can include Forms 1040, 941, 1120 and other informational forms, such as 1099 or W-2.

Data and Information Types: Sensitive
Any information and data not available to the public via the Freedom of Information Act or the State Open Records Laws SDCL 1-27.

Data and Information Types: Trade Secret
Any scientific or technical information and data, design, process, procedure, formula, pattern, compilation, program, device, method, technique, process, strategic planning information or improvement whether manual or electronic that is:
- Valuable and not generally known to the public, including, but not limited to, workstation software programs;
- Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use;
- The subject of efforts that are reasonable under the circumstances to maintain its secrecy, see SDCL 1-27-30

Database
An organized collection of data that supports the processing of the data to provide information.

Data Breach
The unauthorized access by a non-authorized person(s) that result in the use, disclosure, corruption, or theft of State's data.

Data Mining
The analysis of a data base to extract patterns that can be used to learn more about the user; usually used for marketing purposes

Dataset
A collection of related sets of information and data that is composed of separate elements but can be manipulated as a unit by a workstation.

DDN Intranet
The private, internal network of State government. Executive, judicial branch and constitutional offices connect to the internal aspect of the DDN. The DMZ, K12, REED are examples of external aspects of the DDN.

De-Militarized Zone (DMZ)
A perimeter network that contains external-network facing services. Applications needing access from the public Internet are located in the DMZ.

Digital Dakota Network (DDN)
The name of the Statewide workstation network including, but not limited to, data, video, and VoIP services that connects many entities together, including the local and wide area networks of the Executive & Judicial branches, K12 schools and Board of Regents.

Directory
The service that identifies all resources on a network and makes them accessible to users and applications. Resources include e-mail addresses, computers, and peripheral devices such as printers. The directory service allows a user on a network to access any resource without knowing where or how it is physically connected.

Distributed Denial of Service (DDOS)
A botnet is a series of computers compromised. A DDOS attack utilizes one or more botnets to target a single computer or website. The massive amount of botnet traffic overloads the recipient with more data than it can handle, resulting in service delays or outages. The counts indicate the number of attacks targeting the Board of Regents, K12 public schools and State government.

Domain Name
A name owned by a person or organization and consisting of an alphabetical or alphanumeric sequence followed by a suffix. It is used as an Internet address to identify the location of specific Web pages.

Dynamic Naming System (DNS)
An automated means of translating Internet URLs into the equivalent IP address (translating web addresses from near-English into the URL's digital address).

Easter Egg
A secret message buried in an application.

Employee
Anyone employed directly by the State of South Dakota or employed by any third-party company (contractor or subcontractor) that has a contract to provide work for a State government agency. Contractors and Employees are treated identically throughout the Information Technology Security Policy.

End User Data
Data that is not state data but is non-public or personal data provided by an entity other than the state and is used by someone other than the state.

External Network
Any network that resides outside of the established security perimeter.

Extranet
A controlled private network that allows access to an authorized set of customers.

Fail Over
The process that takes place when a computing resource fails, and the functions are automatically moved to another computing resource.

Federal Parent Locator System (FPLS)
The FPLS is an assembly of systems operated by Office of Child Support Enforcement (OCSE), to assist states in locating noncustodial parents, putative fathers, and custodial parties for the establishment of paternity and child support obligations, as well as the enforcement and modification of orders for child support, custody, and visitation. It also identifies support orders or support cases involving the same parties in different states. The FPLS helps federal and state agencies identify over-payments and fraud and assists with assessing benefits.

Federal Tax Information (FTI)
Tax returns or tax return information received from the IRS or secondary source. Information, including the return, that IRS obtained from any source or developed through any means that relates to the potential liability of any person for any tax, penalty, interest, fine, forfeiture, or other imposition or offense and (2) Information extracted from a return, including names of dependents or the (2) location of business (3) The taxpayer's name, address, and identification number (4) Information collected by the IRS about any person's tax affairs, even if identifiers, such as name, address, and identification number are deleted.

File Transfer Protocol (FTP)
A standard network protocol used to transfer data files between one workstation network and another.

Firewall
A set of related programs, located on a state network gateway server that protects the resources of the state's network from un-authorized users from other networks.

Hackers
Individuals or a group of individuals with the intent of doing harm to state data, infrastructure, or services.

Hot Spot
A physical location where people may obtain Internet access.

Hypervisor
A program that is running one or more virtual machines on a single physical server. *See also virtualization.*

Identity Theft
When a hacker gains access to enough personal information about someone that they can impersonate one to acquire financing in that person's name or can gain access to data networks as that person.

Inbound Traffic
Network traffic that originates outside of the enterprise network with a destination inside the network.

Individually Identifiable Health Information (Also known as Personal or Personally Identifiable Health Information)
Is information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Information system
A computer, storage, networking and other physical devices, infrastructure, and processes to create, process, store, secure and exchange all forms of electronic data.

Infrastructure
The technology (hardware and software) that comprise the computer network, phone network, and connections to the Internet including the computer and storage environments.

Infrastructure-as-a-Service
The capability provided to the state to provision, process, and store networks and other fundamental deployments and run arbitrary software, which can include operating systems and applications. The state does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed application; and possibly limited control of select networking components, for example, host firewalls.

Internet of Things (IoT)
The Internet of things (***IoT***) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to connect and exchange data.

IP Address
The address of a connected device on the State's IP network. Every desktop and laptop computer, server, scanner, printer, modem, router, smartphone, and tablet is assigned an IP address.

Load Balancing
Dividing the amount of work that a computer has to do between two or more computers so that more work gets done in the same amount of time and, in general, all users get served faster.

MAC Address
A 12-digit hexadecimal address that is preprogrammed into a computer's network adapter that uniquely identifies that computer on the network.

Malicious Phishing
Email messages disguised to entice the user to enter personal information, network, or banking account information. This information will be sent to the attacker who will use it to steal the user's identity, money, or to access the state network using the user's network log-in information to steal data. State Facilitated Phishing is internal phishing of employees to test and evaluate our education and training efforts.

Malicious Software
A program that gives a hacker control of your computer.

Malware
A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim.

Metadata
Data that describes other data. For example, the date modified field in a listing of files is metadata.

Mobile Applications
Applications running on a mobile device like a smart phone or tablet.

Mobile Device
A portable, wireless computing device that is small enough to be used while held in the hand.

Mobile Wi-Fi
A wireless router that acts as a mobile wireless network outbound spot.

NATURAL
A programming language created by Software AG used to interface with ADABAS (Adaptable Data Base System).

Network
A group of computer systems and hardware devices linked together to facilitate the communication between the devices, the sharing of resources, and that make the exchange of information easier.

Non-Public Data
Data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the State because it contains information that is exempt by statute, ordinance, or administrative rule from access by the general public as public information.

On Premise
The IT infrastructure, applications or data that is located at State facilities. Cloud services, SaaS, PaaS, and IaaS would not be considered to be on premise.

Open Source
Software where the copyright holder allows anyone to study, change and distribute the software to anyone for any purpose without paying a licensing fee.

Operating System
A program that controls the operation of a computer and directs the processing of other programs.

Outbound Traffic
This is traffic that originates inside an enterprise network and has a destination outside of the network.

Payment Card Industry (PCI)
Credit card security specifications created by the credit card industry.

Peripherals
Devices that are utilized to enter data and information into a workstation or retrieve data and information from a workstation.

Personally Identifiable Information (PII)
Data that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information (PII): government-issued identification numbers, for example, Social Security, driver's license, and passport numbers. PII also includes financial account information, including account number, credit or debit card numbers, or protected health information (PHI) relating to a person.

Platform
The type of computer system the network is running on. The state has three; the Windows based platform, the mainframe system, and the AS 400 system.

Platform-as-a-Service (PaaS)
The capability provided to the state to deploy onto the cloud infrastructure state-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The state does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Portable Device
Any computing device that can easily be carried that is designed to be held and used in the hands. Portable devices include laptops, tablets, and smartphones. A portable device may also be called a handheld device or mobile device. *See also Remote Access Device (RAD).*

Portable storage device
A computer media storage device that is capable of being physically transported, including but not limited to USB/flash drives/thumb drives, external hard drives, tapes, CDs, DVDs, and cameras.

Power over Ethernet (POE) switches
A network switch that has Power over Ethernet injection built in.

Presentation Layers
The layer that translates between multiple data formats used by computers that are trying to communicate. The internal communication functions of a computer system are conceptualized by being partitioned into layers, each layer having different functions.

Processor
The actual circuit that processes the instructions that drive a computer.

Production Environment
The setting where applications are run using actual client data as opposed to test environment which is the setting where applications are run using test data.

Program
A sequence of instructions that can be interpreted and executed by a computer.

Protected Data
Data protected by any law, regulation, or industry standard.

Protected Health Information (PHI)
Individually identifiable health information that is:

- Transmitted by electronic media.
- Maintained in electronic media.
- Transmitted or maintained in any other form or medium.

PHI excludes individually identifiable health information in:

- Education records covered by the Family Educational Rights and Privacy Act
- Employment records held by a covered entity in its role as employer.

PHI includes but is not limited to the patient's name, address, patient's doctor, patient's clinic, diagnosis, and prescribed medication.

Reaccreditation
The periodic rescanning of a system looking for security vulnerabilities.

Relative Pathing
A location that is relative to the current directory or folder. By making pathing relative rather than hard coded in an application is less likely to "break" the application because it is looking for a location that has been changed.

Remote Access Device (RAD)
RADs include smartphones like iPhones, Windows, and Android phones; mobile computing devices like iPods, iPads, and notebooks; as well as other non-state workstations such as public access terminals located in libraries, schools and airports or any other internet capable computing device that is mobile or outside the management of BIT. This list is not inclusive.

Resource Access Control Facility (RACF)
An IBM software product. It is a security system that provides access control and auditing functionality for the z/OS and z/VM operating systems.

Rouge Access Point
A wireless access point (WAP) that has been installed on a secure network without authorization.

Router
A networking device that forwards data packets between computer networks.

Sanitization
A process by which data is irreversibly removed from media or the media is permanently destroyed.

Script
A list of commands used by a program to automate processes on a computer.

Security Activity
Activity meant to enhance and maintain a high level of security. This includes scanning network and email communications with sources and destinations that are outside of the state network. It also includes installing upgraded security software and hardware including: anti- virus software, firewalls, content-filtering software, and intrusion detection software.

Security Incident
A violation of any BIT security policies, privacy policies, or contract agreements involving sensitive information, or the imminent threat of a violation.

Security Infrastructure Team (SIT)
The BIT SIT shall, in coordination with the CISO, recommend technology solutions, written policies and procedures necessary for assuring the security and integrity of State information technology.

Security Operations Team (SOT)
The BIT SOT meets daily to review any cyber security findings or issues with the State Infrastructure within the previous day.

Server
A computer that contains a program that awaits and fulfills requests from other programs in the same or other computers. A given application in a computer may function as a source of requests for services from other programs and also as a server of requests from to other programs.

Service Level Agreement
A written agreement between both the State and the Vendor that is subject to the terms and conditions in this document that unless otherwise agreed to includes (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) security responsibilities and notice requirements, (5) how disputes are discovered and addressed, and (6) any remedies for performance failures.

SIM card
A smart card that stores a subscriber's personal identifier, billing information, and data.

Software-as-a-Service (SaaS)
Refers to the capability provided to the State to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The State does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Software Development Life Cycle (SDLC)
A software development methodology used by BIT.

State
Refers to the government of the State of South Dakota when capitalized.

State Contact
The person or persons designated in writing by the State to receive general project communications, adverse event notifications, security incident notifications, or breach notifications.

State Data
Means all data created or in any way originating with the State, and all data that is the output of computer processing

of or other electronic manipulation of any data that was created by or in any way originated with the State, whether such data or output is stored on the State's hardware, the Vendor's hardware or exists in any system owned, maintained, or otherwise controlled by the State or by the Vendor.

State Proprietary Information
The state data plus any other record, information, or document, in any format, that originated with the state.

Statement of Work
A written statement in a solicitation document or contract that describes the State's service requirements.

Structure Query Language
A computer language that is used to manage data, where the data is presented as a set of related tables, and to make queries of a database.

Social engineering
Manipulating individuals to provide confidential information or access to a secured site. Purposely "conning" individuals for the purpose of obtaining information to allow for nefarious cyber activities. The tendency of our culture in SD is to be helpful and thus makes us very vulnerable to being socially engineered.

Software patches
Changes made to applications to fix security vulnerabilities or impaired functionality.

Spoofing
Refers to various practices that conceal the identity of a user account, an email account, or a computer's Internet Protocol (IP) address that is taking some action. For example, email spoofing involves forging the header of an email message so that the message appears to come from someone other than the true sender.

System
A set of interrelating or interdependent component parts forming framework, either software or hardware, connected together to facilitate the flow of data or information.

Test Environment
The setting where applications are run using test data as opposed to production environment which is the setting were applications are run using actual client data.

Time Bomb
A program that will stop functioning once a set time is reached.

Trojan Horse
A malicious program that gives a hacker access to a computer system were the program is disguised as something safe but hides a malicious program.

User Identification (UID)
A user, identifier, or account utilized for access control to specify which technical assets and resources an individual or entity can access. Examples are:

- USERID
- A User ID
- SD Domain Account

Virtual Private Network (VPN)
A method to encrypt data that is sent or received over the public Internet.

Virtualization
The creation of a virtual version of something, such as an operating system, a server, a storage device, or network resources. By allowing multiple virtual versions of something on the same physical server more efficient use is made of network resources.

Web Probing
An intelligence gathering effort to gather background information and to identify configuration files and directories of servers providing web content.

Web Server
A computer that acts as a server that serves up Web pages and applications.

Web Server attacks
Attacks against the servers that connect the state network to the Internet as well as servers that host (store and run) websites. These attacks can be to access data that is not meant to be accessible through the websites via direct probes and software injections from malicious hosts. They can also be meant to prevent users from accessing the websites or the servers. Incidents is the number of successful compromises and Hack Scans are the number of infiltration attempts.

Wi-Fi
The 802.11b standard for wireless networking. A standard for delivering digital information over high-frequency, wireless local area networks.

Wireless Access Point (WAP)
A networking hardware device that allows a Wi-Fi device to connect to a wired network.

Wiring closet
A small room commonly found in institutional buildings where electrical connections are made.

Workstations
Any State-owned desktop, laptop, or tablet computer.

Worm
A malicious program that reproduces itself, so it can spread from one computer to others.

ACRONYMS

ACL
Access Control List

ADABAS
Adaptable Data Base System

BA
Business Associate

BAA
Business Associate Agreement

BHR
South Dakota Bureau of Human Resources

BIT
Bureau of Information & Telecommunications

CISO
Chief Information Security Officer

COTS
Commercial off the Shelf Software

DBMS
Database Management System

DDN
Digital Dakota Network

DDOS
Distributed Denial of Service

DHCP
Dynamic Host Configuration Protocol

DMZ
De-Militarized Zone

DNS
Dynamic Naming System

DOH
South Dakota Department of Health

DSN
Data Source Name

DSS
South Dakota Department of Social Services

EAR
Export Administration Regulations

FERPA
Family Educational Rights and Privacy Act

FPLS
Federal Parent Locator System

FTI
Federal Tax Information

FTP

File Transfer Protocol

GLBA
Gramm-Leach Bliley/ Financial Services Modernization Act

HIPAA
Health Information Portability and Accountability Act

IaaS
Infrastructure as a Service

IEEE
Institute of Electrical and Electronics Engineers

IoT
Internet of Things

IPv4
Internet Protocol version 4

IPv6
Internet Protocol version 6

IRS
Internal Revenue Service

ITAR
International Traffic in Arms Regulations

MANET
Mobile Ad Hoc Network

MIFI
Mobile Wi-Fi

MMIS
Medicaid Management Information System

MOU
Memorandum of Understanding

NIST
National Institute of Standards and Technology

OWASP
Open Web Application Security Project

PaaS
Platform-as-a-Service

PCI
Payment Card Industry

PII
Personally Identifiable Information

RAD
Remote Access Device

RADIUS
Remote Authentication Dial-In User Service

SaaS
Software-as-a-Service

SDLC
Software Development Life Cycle

SLA
Service Level Agreement

SNMP
Simple Network Management Protocol

SOC
Security Operations Center

SOT
Security Operations Team

SOW
Statement of Work

SSID
Service Set Identifier

SQL
Structure Query Language

TACACS+
Terminal Access Controller Access-Control System Plus

UAT
User Assurance Testing

UID
User Identification

VOIP
Voice Over Internet Protocol

VPN
Virtual Private Network

WAN
Wide Area Network

WANET
Wireless Ad Hoc Network

WAP
Wireless Access Point

Attachment B – Cost Proposal

STATE OF SOUTH DAKOTA
DEPARTMENT OF SOCIAL SERVICES
COST PROPOSAL

COST CALCULATION	RESPONSE	MULTIPLY BY	TOTAL COST
Cost per *individual line*		480,000	
Other costs (Describe)			
Annual maintenance cost			
ANNUAL COST			**$**

Attachment C – BIT Permission to Scan

The Consultant acknowledges that the State will conduct a security and vulnerability scan as part of the review of the Consultant's RFP. This scan will not include a penetration test. The State will use commercially available, industry standard tools to scan a non-production environment with non-production data at mutually agreeable times.

The Consultant should fill in the information below and sign the form. The Consultant's employee signing this form must have the authority to allow the State to do a security scan. If no security contact is given the State will assume that the State can scan at any time. **At the state's option, any RFP response that does not include a completed and signed form may be dropped from consideration. If there is State data protected by federal or state law or regulation or industry standard involved the State is more likely to consider a security scan necessary for a RFP to be considered.** Except for State staff the State will only provide scan information to the Consultant's security contact. At the State's option, the State will conduct the scan at a location named by the Consultant. The Consultant can only request, not require naming the scanning location. The State may consider a comprehensive, complete and recent risk assessment as satisfying the scanning requirement. If required, the State will sign a non-disclosure agreement before scanning or receiving the risk assessment.

Consultant's name: _____

Consultant's security contact's name: _____

Security contact's phone number: _____

Security contact's email address: _____

Web address URL or Product Name _____
The State will contact the security contact to arrange for a test log for scanning.

Consultant's employee acknowledging the right to scan (Print): _____

Title: _____

Date: _____

Signature: _____

Intentionally left blank

Attachment D

Security and Vendor Questions

Agencies: The following questions help agencies acquire technology that meets state security and technology standards. BIT recommends that you contact your BIT Point of Contact to arrange a meeting if you have questions regarding this questionnaire or how it relates to your project.

It is rarely possible to know ahead of time the details of the technologies a vendor will propose. For this reason, you will get the best outcome if the questions remain as-is. Vendors are invited to mark those questions that do not apply to their set of technologies with NA (Not Applicable). In the rare case when there is detailed knowledge of what will be proposed beforehand, a narrowed set of questions may be possible, contact your BIT Point of Contact if you have questions about this.

Vendors: The following questions help the state determine the best way to assess your product or service technology for appropriate fit with the state's technology needs. Some questions may not apply to the technology you use. In such cases, mark the question as NA (Not Applicable). Use the last column as needed to explain your answers. Questions with the Yes/No cells greyed out require you to explain your response. The more detailed the response, the better we can understand your product and/or service.

The "BIT" column corresponds to the branch that will be the primary reviewers. If you have questions about the meaning or intent of a question, we can contact them on your behalf. DAT = Data Center; DEV = Development; TEL = Telecommunications; PMO = Project Management office

Section A: System Security

The following questions are relevant for all vendors or third-parties engaged in this application or service, and pertain to relevant security practices and procedures for your system and coding.

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
A1	DAT	Is a user required to change their password? How often? What are the complexity requirements for the passwords? (BIT password requirements are available in Section 230.67.4.4 of the Information Technology Security Policy which can be supplied upon request).				
A2	DEV TEL	Will the system implement its own level of security?				
A3	DAT TEL x	Will the system provide Internet security functionality on public portals using encrypted network/secure socket layer connections in line with current recommendations of the Open Web Application Security Project (OWASP)?				

A4	TEL x	Will the system provide Internet security functionality on a public portal to include firewalls?				
A5	PMO	Will the system distinguish between local versus global administrators where local administrators have rights to user management only for the program area that they are associated with and global administrators have rights for the entire system?				
A6	DAT TEL	Does the application contain mitigations for risks associated to uncontrolled login attempts (response latency, re-Captcha, lockout, IP filtering, Multi Factor authentication)? Which mitigations are in place? What are the optional mitigations?				
A7	DAT TEL	Are account credentials hashed and encrypted when stored?				
A8	DAT TEL x	The protection of the State's system and data is of upmost importance. Security scans must be done if: · An application will be placed on the State's system; · The State's system connects to another system; · The vendor stores or processes State data. **The State would want to scan a test system; not a production system and will not do penetration testing.** The scanning will be done with industry standard tools. Scanning would also take place annually as well as when there are code changes. Is any of this an issue? If so, please explain.				
A9	DAT	Will SSL traffic be decrypted and inspected?				
A10	PMO x	Will organizations other than the State of South Dakota have access to our data?				
A11	PMO	Will the State's data be protected?				
A12	DEV TEL	Describe the training your company offers related to defining security requirements, secure architecture and design, secure coding practices, and security testing.				

A13	DEV TEL	Do you have developers that possess software security related certifications (e.g., the SANS secure coding certifications)?				
A14	DEV	Are there some requirements for security that are "structured" as part of general releasability of a product and others that are "as needed" or "custom" for a particular release?				
A15	TEL	What process is utilized by your company to prioritize security related enhancement requests?				
A16	TEL	What threat assumptions were made, if any, when designing protections for the software and information assets processed?				
A17	TEL	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used?				
A18	TEL	What security criteria, if any, are considered when selecting third-party suppliers?				
A19	TEL	How has the software been measured/assessed for its resistance to identified, relevant attack patterns such as Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumerations (CWEs)? How have the findings been mitigated?				
A20	TEL	Has the software been evaluated against the Common Criteria, FIPS 140-2, or other formal evaluation process? If so, please describe what evaluation assurance level (EAL) was achieved, what protection profile the product claims conformance to, and indicate if the security target and evaluation report are available.				
A21	DAT TEL	Are static or dynamic software security analysis tools used to identify weaknesses in the software that can lead to exploitable vulnerabilities? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?				
A22	DAT TEL x	Has the product undergone any penetration testing? If yes, when, by whom, and are the test reports available under a nondisclosure agreement? How have the findings been mitigated?				
A23	DEV	Are there current publicly-known vulnerabilities in the software (e.g., an unrepaired CWE entry)? If yes, please explain.				

A24	DAT	Does your company publish a security section on its website? If so, do security researchers have the ability to report security issues?				
A25	DAT	Does your company have an executive-level officer responsible for the security of your company's software products and/or processes?				
A26	DAT	Are security requirements developed independently of the rest of the requirements engineering activities? Or are they integrated into the mainstream requirements activities?				
A27	DAT	Does the software have any security critical dependencies or need additional controls from other software (e.g., operating system, directory service, application), firmware, or hardware? If yes, please describe.				
A28	DAT	What risk management measures are used during the software's design to mitigate risks posed by use of third-party components?				
A29	DAT	Does your company perform background checks on members of the software development team? If so, are there any additional "vetting" checks done on people who work on critical application components, such as security? Explain.				
A30	DEV	Does your company have formally defined security policies associated with clearly defined roles and responsibilities for personnel working within the software development life cycle? Explain.				
A31	TEL	What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?				
A32	DAT	Is two-factor authentication used for administrative control of all security devices and critical information systems?				
A33	DAT TEL	Do you have an automated security event management system?				
A34	DAT	Are security logs and audit trails protected from tampering or modification?				
A35	DAT	It is State policy that if your system connects to another system providing SaaS, IaaS, or PaaS that this system has a security scan. The State would want to scan a test system; not a production system. Is this an issue? If so, please explain.				

A36	DAT x	A) Will the system support authentication?				
		B) Does the system give clues about valid username or password content or structure, for example when a user forgets their username or after a failed login attempt?				
		C) Are usernames and passwords generated by the system using user-specific information such as last name or birthdate?				
		If Yes to these, please explain.				
A37	DEV	Are security-specific regression tests performed during the development process? If yes, how frequently are the tests performed?				
A38	TEL	What type of firewalls (or application gateways) do you use? How are they monitored/managed?				
A39	TEL	What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they monitored/managed?				
A40	DAT TEL	What are your procedures for intrusion detection, incident response, and incident investigation/escalation?				
A41	DAT	How do you control physical and electronic access to the log files? Are log files consolidated to single servers?				
A42	DAT TEL	Describe your security testing processes.				
A43	DAT TEL	Do you have a BYOD policy that allows your staff to put any sort of sensitive or legally protected State data on their device personal device(s) or other non-company owned system(s)?				
A44	DAT TEL	Do you require multifactor authentication be used by employees and subcontractors who have potential access to legally protected State data? If yes, please explain your practices on multifactor authentication including the authentication level used as defined in NIST 800-63 in your explanation. If no, do you plan on going to multifunction authentication? If so, when?				
A45	PMO	Will this system provide the capability to track data entry/access by the person, date and time?				

A46	DAT DEV PMO TEL	Will the system provide data encryption for sensitive or legally protected information both at rest and transmission? If yes, please provide details.				
A47	DAT	a. Do you have a SOC 2 audit report?				
		b. Is the audit done annually?				
		c. Does the audit cover all 5 of the trust principles?				
		d. Does the audit include subservice providers?				
		e. Has the auditor always been able to attest to an acceptable audit result?				
		f. Will you provide a copy of your latest SOC 2 audit upon request, a redacted version is acceptable.				
A48	DAT TEL	Are you providing a device or software that is a part of the Internet of Things (IoT)? If yes, what is your process for ensuring the software on your IoT devices that are connected to the state's system, either permanently or intermittently, are maintained and/or updated?				

Section B: Hosting

Only for Vendor hosted applications, systems, databases, services and any other technology not hosted on the State's infrastructure. Mark the questions as "NA" if this is an application hosted by the State.

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
B1	PMO	Typically the State of South Dakota prefers to host all systems. In the event that the State decides that it would be preferable for the vendor to host the system, is this an option?				
B2	PMO	Are there expected periods of time where the application will be unavailable for use?				
B3	DAT	If you have agents or scripts executing on servers of hosted applications and what are the procedures for reviewing the security of these scripts or agents?				
B4	DAT	What are the procedures and policies used to control access to the servers? How are audit logs maintained?				

B5	DAT DEV PMO TEL	Do you have a formal disaster recovery plan? Please explain what actions will be taken to recover from a disaster? Are warm or hot backups available?				
B6	DAT	What are the set of controls to ensure separation of data and security information between different customers that are physically located in the same data center? On the same host server?				
B7	DAT	What are your data backup policies and procedures? How frequently are your backup procedures verified?				
B8	DAT	Are you or if the data is being hosted by a subservice provider are they FedRAMP certified?				
B9	DAT DEV TEL	If any cloud services are provided by a third-party, do you have contractual requirements with them dealing with: · Security for their I/T systems; · Staff vetting; · Staff security training?				
		If yes, summarize the contractual requirements.				
		If yes, how do you evaluate the third-party's adherence to the contractual requirements?				
B10	DAT	If your application is hosted by you or a third party, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal? If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?				
B11	DAT	a. Do you use a security checklist when standing up any outward facing system?				
		b. Do you test after the system was stood up to make sure everything in the checklist was correctly set?				
		c. Will you provide the State with a copy of your checklist?				
B12	DAT	Are your Internet of Things (IoT) devices segmented from your network?				

Section C: Database

Applies to any application or service that stores data, regardless of the application being hosted by the state or the vendor.

			Response			
#	BIT	Question	YES	NO	NA	Explanation
C1	DAT	Will the system require a database?				
C2	DAT	Will the system infrastructure require database replication?				
C3	DAT	Will the system require transaction logging for database recovery?				
C4	DAT DEV	How does data enter the system (transactional or batch or both)?				
C5	PMO	Is the system data exportable by the user for use in tools like Excel or Access?				
C6	PMO	Will user customizable data elements be exportable also?				
C7	DAT DEV PMO	Will the State of South Dakota have access to the underlying data and data model for ad hoc reporting purposes? If yes, will the access be on-site or off-site?				
C8	DAT DEV	Will the system infrastructure include a separate OLTP or Data Warehouse Implementation?				
C9	DAT DEV	Will the system infrastructure require a Business Intelligence solution?				

Section D: Vendor Process

The following questions are relevant for all vendors or third-parties engaged in this application or service and pertain to business practices. If the application is hosted by the vendor or the vendor supplies cloud services those questions dealing with installation or support of applications on the State's system can be marked "NA".

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed

D1	DAT PMO	Will the vendor provide assistance with installation?				
D2	DAT DEV PMO TEL	Does your company have a policy and process for supporting/requiring professional certifications? If so, how do you ensure certifications are valid and up-to date?				
D3	TEL	In preparation for release, are undocumented functions in the software disabled, test/debug code removed, and source code comments sanitized?				
D4	DEV	What types of functional tests are/were performed on the software during its development (e.g., spot checking, component-level testing and integrated testing)?				
D5	TEL	Who and when are security tests performed on the product? Are tests performed by an internal test team, by an independent third party, or by both?				
D6	DEV	Are misuse test cases included to exercise potential abuse scenarios of the software?				
D7	TEL	What release criteria does your company have for its products with regard to security?				
D8	DEV	What controls are in place to ensure that only the accepted/released software is placed on media for distribution?				
D9	DAT DEV	Is there a Support Lifecycle Policy within the organization for the software in question? Does it outline and establish a consistent and predictable support timeline?				
D10	DAT	How will patches and/or Service Packs be distributed to the Acquirer?				
D11	DEV	What services does the help desk, support center, or (if applicable) online support system offer and when are these services available?				
D12	DAT DEV	How extensively are patches and Service Packs tested before they are released?				
D13	DAT	Can patches and Service Packs be uninstalled? Are the procedures for uninstalling a patch or Service Pack automated or manual?				

D14	DAT DEV	How are reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, and prioritized?				
D15	DAT	How do you set the relative severity of defects and how do you prioritize their remediation?				
D16	DAT	What are your policies and practices for reviewing design and architecture security impacts in relation to deploying patches?				
D17	DAT	Are third-party developers contractually required to follow your configuration management policies?				
D18	DEV	What policies and processes does your company use to verify that software components do not contain unintended, "dead," or malicious code? What tools are used?				
D19	DEV	How is the software provenance verified (e.g. any checksums or signatures)?				
D20	DEV	Does the documentation explain how to install, configure, and/or use the software securely? Does it identify options that should not normally be used because they create security weaknesses?				
D21	DAT	Does your company's defect classification scheme include security categories?				
D22	DAT	Is a validation test suite or diagnostic available to validate that the application software is operating correctly and in a secure configuration following installation?				
D23	DEV	Does your company develop security measurement objectives for phases of the SDLC? Has your company identified specific statistical and/or qualitative analytical techniques for measuring attainment of security measures?				
D24	DEV	How is the assurance of software produced by third-party developers assessed?				
D25	DEV	Does your company have a vulnerability management and reporting policy? Is it available for review?				
D26	DAT	What are the procedures for evaluating any vendor security alerts and installing patches and Service Packs?				

D27	DAT	Is testing done after changes are made to servers? What are your rollback procedures in the event of problems resulting from installing a patch or Service Pack?				
D28	DAT	What are your procedures and policies for handling and destroying sensitive data on electronic and printed media?				
D29	DAT TEL	How are virus prevention, detection, correction, and updates handled for the products?				
D30	DAT TEL	Do you perform regular reviews of system and network logs for security issues?				
D31	DAT	Do you provide security performance measures to the customer at regular intervals?				
D32	DAT PMO	Is there an installation guide available and will you provide a copy to the State?				
D33	DAT DEV PMO	Will the implementation plan include user acceptance testing?				
D34	DAT DEV PMO TEL	Will the implementation plan include performance testing?				
D35	DAT DEV PMO TEL	What technical documentation will be provided to the State?				
D36	DEV PMO	Will there be documented test cases for future releases including any customizations done for the State of South Dakota?				
D37	PMO	Is the user manual electronically available and can the manual be printed?				
D38	PMO	Describe your Support and on-line assistance options and any additional costs associated with the options.				
D39	DAT PMO	Is there a method established to communicate availability of system updates?				

D40	DEV PMO	If the State of South Dakota will gain ownership of the software, does the proposal include a knowledge transfer plan?				
D41	DEV PMO	Has your company ever conducted a project where your product was load tested?				
D42	DEV PMO	Have you ever created a User Acceptance Test plan and test cases? If yes, what were the test cases? Do you do software assurance?				
D43	PMO	Is there a strategy for mitigating unplanned disruptions and what is it?				
D44	DAT	Please explain the pedigree of the software. Include in your answer who are the people, organization and processes that created the software.				
D45	DAT	Explain the change management procedure used to identify the type and extent of changes allowed in the software throughout its lifecycle. Include information on the oversight controls for the change management procedure.				
D46	TEL	Does your company have corporate policies and management controls in place to ensure that only corporate-approved (licensed and vetted) software components are used during the development process? Provide a brief explanation. Will the supplier indemnify the Acquirer from these issues in the license agreement? Provide a brief explanation.				
D47	DEV	What are the processes (e.g., ISO 9000, CMMi), methods, tools (e.g., IDEs, compilers) techniques, etc. used to produce and transform the software (brief summary response)?				
D48	DAT DEV	Does the software contain third-party developed components? If yes, are those components scanned by a static code analysis tool?				
D49	DAT DEV TEL	What security design and security architecture documents are prepared as part of the SDLC process? How are they maintained? Are they available to/for review?				
D50	DEV	Does your organization incorporate security risk management activities as part of your software development methodology? If yes, please provide a copy of this methodology or provide information on how to obtain it from a publicly accessible source.				

D51	DAT	Does the organization ever perform site inspections/policy compliance audits of its U.S. development facilities? Of its non-U.S. facilities? Of the facilities of its third-party developers? If yes, how often do these inspections/audits occur? Are they periodic or triggered by events (or both)? If triggered by events, provide examples of "trigger" events.				
D52	DEV	When does security testing occur during the SDLC (e.g., unit level, subsystem, system, certification and accreditation)?				
D53	DAT TEL	How are trouble tickets submitted? How are support issues, specifically those that are security-related escalated?				
D54	DAT TEL	Do you perform penetration testing of the service? If yes, how frequently are penetration tests performed? Are the tests performed by internal resources or by a third party?				
D55	DAT	How frequently is the security tests performed? Are the tests performed by internal resources or by a third party?				
D56	DAT DEV	Please describe the scope and give an overview of the content of the security training you require of your staff, include how often the training is given and to whom.				
D57	DAT TEL	What is your process for ensuring the software on your IoT devices that are connected to your system, either permanently or intermittently, is maintained and updated?				
D58	DAT TEL x	It is State policy that all Vendor/Contractor Remote Access to systems for support and maintenance on the State Network will only be allowed through Citrix Netscaler. Would this affect the implementation of the system?				
D59	PMO TEL x	The Vendors/Contractors are also expected to reply to follow-up questions in response to the answers they provided to the security questions. At the State's discretion, a vendor's answers to the follow-up questions may be required in writing and/or verbally. The answers provided may be used as part of the vendor selection criteria. Is this acceptable?				

D60	DAT DEV PMO TEL x	(For PHI only) a. Have you done a risk assessment? If yes, will you share it?				
		b. If you have not done a risk assessment, would you be willing to do one based on the Health and Human Services assessment tool (https://www.healthit.gov/providers-professionals/security-risk-assessment-tool)? If yes, will you share it? The State is willing to sign a Non-disclosure Agreement before viewing any risk assessment.				
		c. If you have not done a risk assessment, when are you planning on doing one?				
D61	DEV PMO	Will your web site and/or web application conform to the accessibility requirements of the Web Content Accessibility Guidelines 2.0? If not discuss what steps you take to make your web site and/or web application accessible. The guidelines can be found at http://www.w3.org/TR/WCAG20/.				

Section E: Software Development

The following questions pertain to the tools and third-party components used to develop your application, regardless of the application being hosted by the State or the vendor

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
E1	DEV PMO x	What is the development technologies used for this system? Please indicate version as appropriate				
		ASP.Net				
		VB.Net				
		C#.Net				
		.NET Framework				

		Java/JSP				
		MS SQL				
E2	DAT TEL	Is this a browser based User Interface?				
E3	DEV PMO	Will the system have any workflow requirements?				
E4	DAT	Can the system be implemented via Citrix?				
E5	DAT	Will the system print to a Citrix compatible networked printer?				
E6	TEL	If your application does not run under the latest Microsoft operating system, what is your process for updating the application?				
E7	DEV	Identify each of the Data, Business and Presentation layer technologies your product would use and provide a roadmap outlining how your release and or update roadmap aligns with the release and or update roadmap for this technology.				
E8	TELx	Will your system use Adobe Air, Adobe Flash, Adobe ColdFusion, Apache Flex, JavaFX, Microsoft Silverlight, PHP or QuickTime? If yes, explain?				
E9	DEV	In order to connect to other applications or data, will the State be required to develop custom interfaces?				
E10	DEV	In order to fulfill the scope of work, will the State be required to develop reports or data extractions from the database? Will you provide any APIs that the State can use?				
E11	DEV PMO	Has your company ever integrated this product with an enterprise service bus to exchange data between diverse computing platforms?				
E12	DAT	If the product is hosted at the State, will there be any third-party application(s) or system(s) installed or embedded to support the product (for example, database software, run libraries)? If so, please list those third-party application(s) or system(s).				
E13	DEV	What coding and/or API standards are used during development of the software?				
E14	DEV	Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented functions?				

E15	DEV	How does the software's exception handling mechanism prevent faults from leaving the software, its resources, and its data (in memory and on disk) in a vulnerable state?				
E16	DEV	Does the exception-handling mechanism provide more than one option for responding to a fault? If so, can the exception handling options be configured by the administrator or overridden?				
E17	DEV	What percentage of code coverage does your testing provide?				
E18	DAT	A) Will the system infrastructure involve the use of email?				
		B) Will the system infrastructure require an interface into the State's email infrastructure?				
		C) Will the system involve the use of bulk email distribution to State users? Client users? In what quantity will emails be sent, and how frequently?				
E19	TEL x	A) Does your application use Java?				
		B) If yes, is it locked into a certain version?				
		C) Will it use the latest version of Java?				
		D) If so, what is your process for updating the application?				
E20	DAT	Explain how and where the software validates (e.g., filter with white listing) inputs from untrusted sources before being used.				
E21	TEL	Has the software been designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user)? Is it designed to isolate and minimize the extent of damage possible by a successful attack?				
E22	TEL	Does the program use run-time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from data memory, and taint checking)?				
E23	DEV	Do you use open source software or libraries? If yes, do you check for vulnerabilities in your software or library that are listed in:				
		a. Common Vulnerabilities and Exposures (CVE) database?				
		b. Open Source Vulnerability Database (OSVDB)?				

		c. Open Web Application Security Project (OWASP) Top Ten?				

Section F: Infrastructure

This pertains to how your system interacts with the State's technology infrastructure. If the proposed technology does not interact with the State's system the questions can be marked as "NA".

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
F1	TEL	Is there a workstation install requirement?				
F2	DAT	Will the system infrastructure have a special backup requirement?				
F3	DAT	Will the system infrastructure have any processes that require scheduling?				
F4	DAT	The State expects to be able to move your product without cost for Disaster Recovery purposes and to maintain high availability. Will this be an issue?				
F5	TEL x	Will the network communications meet Institute of Electrical and Electronics Engineers (IEEE) standard TCP/IP (IPv4, IPv6) and use either standard ports or State-defined ports as the State determines?				
F6	DAT x	It is State policy that all systems must be compatible with BIT's dynamic IP addressing solution (DHCP). Would this affect the implementation of the system?				
F7	TEL x	It is State policy that all software must be able to use either standard Internet Protocol ports or Ports as defined by the State of South Dakota BIT Network Technologies. Would this affect the implementation of the system? If yes, explain.				
F8	DAT	It is State policy that all HTTP/SSL communication must be able to be run behind State of South Dakota content switches and SSL accelerators for load balancing and off-loading of SSL encryption. If need is determined by the State, would this affect the implementation of the system? If yes, explain.				

F9	DAT x	The State has a virtualize first policy that requires all new systems to be configured as virtual machines. Would this affect the implementation of the system? If yes, explain.				
F10	TEL x	It is State policy that all access from outside of the State of South Dakota's private network will be limited to set ports as defined by the State and all traffic leaving or entering the State network will be monitored. Would this affect the implementation of the system? If yes, explain.				
F11	TEL	It is State policy that systems must support NAT and PAT running inside the State Network. Would this affect the implementation of the system? If yes, explain.				
F12	TEL x	It is State policy that systems must not use dynamic TCP or UDP ports unless the system is a well-known one that is state firewall supported (FTP, TELNET, HTTP, SSH, etc.). Would this affect the implementation of the system? If yes, explain.				
F13	DAT	The State of South Dakota currently schedules routine maintenance from 0400 to 0700 on Tuesday mornings for our non-mainframe environments and once a month from 0500 to 1200 for our mainframe environment. Systems will be offline during this scheduled maintenance time periods. Will this have a detrimental effect to the system?				
F14	DEV PMO	Does your product run on Citrix Metaframe?				
F15	PMO TEL	Please describe the types and levels of network access your system/application will require. This should include, but not be limited to: TCP/UDP ports used, protocols used, source and destination networks, traffic flow directions, who initiates traffic flow, whether connections are encrypted or not, and types of encryption used. Vendor should specify what access requirements are for user access to the system and what requirements are for any system level processes. Vendor should describe all requirements in details and provide full documentation as to the necessity of the requested access.				
F16	PMO x	List any hardware or software you propose to use that is not State standard, the standards can be found at http://bit.sd.gov/#.				

F17	DAT	If your application is hosted on the State's infrastructure, will it require a dedicated environment?				
F18	DEV PMO	Will the system provide an archival solution? If not, is the State expected to develop a customized archival solution?				
F19	DAT	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?				
F20	DAT	What are your policies and procedures for hardening servers?				
F21	DAT TEL	Explain or provide a diagram of the architecture for the application including security mitigation.				
F22	TEL x	What is your process for ensuring default remote login protocols and default passwords are disabled on Internet of Things (IoT) devices that are connected to your system either permanently or intermittently?				
F23	DAT	Can the system be integrated with our enterprise Active Directory to ensure access is controlled?				
F24	TEL x	It is State policy that no equipment can be connected to State Network without direct approval of BIT Network Technologies. Would this affect the implementation of the system?				
F25	DAT x	Will the server-based software support: a. Windows server 2012 R2				
		b. IIS7.0 or higher				
		c. MS SQL Server 2008R2 or higher				
		d. Exchange 2010 or higher				
		e. Citrix presentation server 4.5 or higher				
		f. VMWare ESXi 5.5 or higher				
		g. MS Windows Updates				
		h. Symantec End Point Protection				
F26	TEL x	All network systems must operate within the current configurations of the State of South Dakota's firewalls, switches, IDS/IPS and desktop security infrastructure. Would this affect the implementation of the system?				

F27	DAT	It is State policy that all systems that require an email interface must leverage existing SMTP processes currently managed by BIT Datacenter. Mail Marshal is the existing product used for SMTP relay. Would this affect the implementation of the system?				
F28	DAT TEL	The State implements enterprise-wide anti-virus solutions on all servers and workstations as well as controls the roll-outs of any and all Microsoft patches based on level of criticality. Do you have any concerns in regards to this process?				
F29	DAT TEL	What physical access do you require to work on hardware?				

Section G: Business Process

These questions relate to how your business model interacts with and meets the State's policies, procedures and practices. If the vendor is hosting the application or providing cloud services questions dealing with installation or support of applications on the State's system can be marked "NA".

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
G1	DAT	If your application is hosted on a dedicated environment within the State's infrastructure, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal?				
		If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?				
G2	PMO	Explain the software licensing model.				
G3	DAT DEV PMO	Is on-site assistance available? If so, is there a charge?				
G4	DEV PMO	Will you provide customization of the system if required by the State of South Dakota?				
		If yes, are there any additional costs for the customization?				

G5	PMO	Will the source code for the system be put in escrow for the State of South Dakota? If yes, will you pay the associated escrow fees?				
G6	PMO	Explain the basis on which pricing could change for the State based on your licensing model.				
G7	PMO	Contractually, how many years price lock are you offering the State as part of your response? Also as part of your response, how many additional years are you offering to limit price increases and by what percent?				
G8	PMO	Will the State of South Dakota own the data created in your hosting environment?				
G9	PMO	Will the State acquire the data at contract conclusion?				
G10	PMO	Will the State's data be used for any other purposes other than South Dakota's usage?				
G11	DAT	Has your company ever filed for Bankruptcy under U.S. Code Chapter 11? If so, please provide dates for each filing and describe the outcome.				
G12	DAT	Has civil legal action ever been filed against your company for delivering or failing to correct defective software? Explain.				
G13	DAT	Please summarize your company's history of ownership, acquisitions, and mergers (both those performed by your company and those to which your company was subjected).				
G14	DAT	Will you provide on-site support 24x7 to resolve security incidents?				
G15	DEV	What training programs, if any, are available or provided through the supplier for the software? Do you offer certification programs for software integrators? Do you offer training materials, books, computer-based training, online educational forums, or sponsor conferences related to the software?				
G16	DAT TEL	Are help desk or support center personnel internal company resources or are these services outsourced to third parties?				
G17	DAT	Are any of the services you plan to use located offshore (examples include data hosting, data processing, help desk and transcription services)?				

G18	DAT	Is the controlling share (51%+) of your company owned by one or more non-U.S. entities?				
G19	DAT	What are your customer confidentiality policies? How are they enforced?				
G20	DAT	Are you ISO 27001 certified? Is the certification done annually? Will you provide a copy of your certification report?				
G21	DAT	(Use if PHI is involved) Are you HITRUST certified? Is the certification done annually? Will you provide a copy of your assessment?				
G22	DAT PMO x	Will this application now or possibly in the future share PHI with other entities on other networks, be sold to another party or be accessed by anyone outside the US?				
G23	DAT	If the product is hosted at the State, will there be a request to include an application to monitor license compliance?				
G24	DAT PMO	Is telephone assistance available for both installation and use? If yes, are there any additional charges?				